THEY MIGHT BE GIANTS: SMALL-SCALE RPAs AS A THREAT TO AIR BASE DEFENSE AND AIR POWER PROJECTION

BY

BERT W. ADAMS

A THESIS PRESENTED TO THE FACULTY OF

THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES

FOR THE COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCE AIR AND SPACE STUDIES

AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2014

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
They Might Be Giants: Small-Scale RPAs As A Threat To Air Base Defense And Air Power Projection	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **School of Advance Air And Space Studies,,Air University,,Maxwell Air Force Base,,AL**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Over the past seventy years, the Department of Defense and its installations came under attack many hundreds of times, demonstrating an inability to defend the air base against harassing standoff attacks. These attacks did not attempt to overthrow, conquer or seize an air base but sought instead to interrupt base operations and sortie generation. By doing so, enemies attempted to blunt the overwhelming power afforded by air power and its resources. This thesis argues that as technology advances, it will afford adversaries enhanced capability to execute precision standoff attacks through commercially available and adaptable small-scale Remotely Piloted Aircraft. This type of aircraft has undergone rapid expansion in capability, now offering longer range greater payload ferrying ability, enhanced navigation by GPS and autonomous flight control systems, and ease of use. Coupled to malicious intent, these factors offer adversaries with an affordable and expendable method of exploiting the air domain without suffering the traditional costs associated with air power assets. Due to the low speed, low detectability, and increasing lethality of small-scale RPAs, a precision attack against high-value assets can successfully interrupt air power projection and the protection of ground forces.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**91**	

APPROVAL

The undersigned certify that this thesis meets the master's level standards of research, argumentation, and expression.

_____

COL MARK O. YEISLEY, COL, USAF (DATE)

_____

DR. STEPHEN D. CHIABOTTI, PhD. (DATE)

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.

ABOUT THE AUTHOR

Major Bert W. Adams graduated from The Citadel in 1999 with a Bachelor of Science degree in Business Administration. He received a Master's of Aerospace Science in Aviation Management from Embry-Riddle Aeronautical University in 2008 and a Master's of Science in National Security and Strategic Studies from the US Navy War College in 2013. His 15-year career as an active duty maintenance officer provided a variety of assignments and duties, including multiple deployments, executive officer tours, and command of the 982d Maintenance Squadron, Sheppard Air Force Base, Texas. He has field and depot-level maintenance experience on C-5, KC-10, and C-17 aircraft as well as multiple General Electric jet and turbofan engines. He takes command of the 730th Air Mobility Squadron at Yokota Air Base, Japan in July 2014.

ACKNOWLEDGEMENTS

I would like to acknowledge several people, for whom this journey would be wholly and incomprehensibly difficult and maybe even impossible. First, my loving wife of so many years who sat patiently by my side with unswerving grace and dignity, giving me pep talks and scolding as each was appropriate to keep me focused. I love and adore you and I cherish your elegance. Next, to my children who began each morning with a singular, ominous, “Is it a work day, Dad?” The frequency of saying yes is a familiar and sad sentiment to SAASS students. While your questions were unfortunate at the time, rest assured that my experience here yields knowledge I hope to bestow to you and others so that all the yes answers become worthwhile. Next, I commend my fellow peers in SAASS Class XXIII whose infinite humor and support proved the power of positive thought, especially in large numbers. Lastly, to my advisor, Col Mark Yeisley. Thank you for your patience and help along the journey. I am better for your involvement. As an aside, I think you should have stomped on my neck much earlier – this product would have been far timelier!

ABSTRACT

Over the past seventy years, the Department of Defense and its installations came under attack many hundreds of times, demonstrating an inability to defend the air base against harassing standoff attacks. These attacks did not attempt to overthrow, conquer, or seize an air base but sought instead to interrupt base operations and sortie generation. By doing so, enemies attempted to blunt the overwhelming power afforded by air power and its resources. This thesis argues that as technology advances, it will afford adversaries enhanced capability to execute precision standoff attacks through commercially available and adaptable small-scale Remotely Piloted Aircraft. This type of aircraft has undergone rapid expansion in capability, now offering longer range, greater payload ferrying ability, enhanced navigation by GPS and autonomous flight control systems, and ease of use. Coupled to malicious intent, these factors offer adversaries with an affordable and expendable method of exploiting the air domain without suffering the traditional costs associated with air power assets. Due to the low speed, low detectability, and increasing lethality of small-scale RPAs, a precision attack against high-value assets can successfully interrupt air power projection and the protection of ground forces.

CONTENTS

Illustrations

Table

Figure

Chapter 1

INTRODUCTION

Introduction

In 1207 the famous conqueror Genghis Khan and his warriors rode nearly 600 miles across the Gobi desert, surviving by drinking milk and the blood of their horses. The warriors of the nearby state of Xi Xia were ill-prepared to battle Khan's army and, caught in the open, became easy prey to the highly disciplined Mongols. Xi Xia's heavily fortified defenses, however, became a significant challenge to Khan and his men, who soon learned the futility of using cavalry against the Xi Xia's fortresses. Unable to breach the walls of Volohai, one of Xi Xia's defensive forts, Khan fell back upon his resourcefulness. In a clever trick, he sent a message to the opposition's general, announcing that he would end the Mongol siege in exchange for 1,000 cats and 10,000 swallows.

The fortress commander, surprised by the simplicity, complied with the request. After the animals arrived in the Mongol camp, Khan had his men tie flammable pieces of cotton and wool tuft to each animal. The men then set fire to the cloth and let the animals loose. Once free, the panicked animals returned to their original nests inside the attics and lairs of the city, igniting hundreds of small fires. While the city residents remained distracted putting out fires, Khan and his men stormed the city in conquest.[1]

There are multiple versions of this story; however, the consistency of its theme lends it credibility. Assuming the story is accurate, it may demonstrate one of history's earliest recorded applications of standoff, precision, and economy of force.[2] As such, these tenets are not new to warfare; they have proven central to battlefield victories from as far back as medieval times when defenders poured hot oil over soldiers attempting to

---

[1] Bill Caraway, "Korea in the Eye of the Tiger: Ch. 5 Koryo and the Mongols, Building an Empire," Korean History Project, April 12, 2014, accessed April 12, 2014, http://www.koreanhistoryproject.org/index.htm.

[2] David Mets, "RPAs: Revolution or Retrogression", *Air Force Research Institute Papers* (paper 2010-1, April 2010): 2.

seize a castle.[3] Not only did this represent standoff, precision, and economy of force, it prevented placing your own troops in peril during the defense.

Over time, these tenets served many nations and kingdoms seeking advantages over their adversary. Generations later, military forces took to the skies when science enabled balloon-delivered ordnance, allowing forces to gain the high ground without risking troops in the process. After balloons, mechanized aircraft hurtled men through the clouds, but put them in harm's way in the exchange. As aircraft and air power later grew in popularity, so did the concepts of taking to the sky in a way that removed the man from the machine. Unfortunately, technology was a bitter foe, preventing many of the earliest unmanned attempts from being effective forms of warfare.

The subsequent advancement of technology over the following decades illustrated an almost logarithmic increase in capability and energized the concepts of unmanned warfare. As the computer age arrived, the axiom of Moore's Law surfaced, which argues that the processing power of computers doubles every two years.[4] If Moore's Law remains relevant for other technologies, then it may have a tangible effect on the rate of change and advancement of small-scale Remotely Piloted Aircraft (RPA). As a result of these advancements, it may alter and improve the methods used by malicious actors seeking harm to the US. This is the central theme of this thesis and builds the foundation for its hypothesis. Specifically, the rapid rate of technological advancement will increase affordability, utility, and availability of small-scale RPAs, creating a cost-effective opportunity for adversaries to exploit the air domain to their advantage and effectively challenge current methods of air base defense and the projection of air power.

Growth and Maturation of RPAs

In the initial stages of aviation, the use of aircraft did not remain isolated to military operations. Over time, civilian applications grew considerably. While the aircraft gained popularity with each passing year, an interesting but subtle development took place: the continued development of unmanned aircraft. At first glance, it may appear odd that unmanned aircraft held any part of the aviation discussion, especially while manned

[3] Mets, 2.
[4] "Moore's Law -- or -- How Overall Processing Power for Computers Will Double Every Two Years," Moore's Law, April 18, 2014, accessed April 18, 2014, http://www.mooreslaw.org/.

platforms grew so quickly in prominence. In truth, as long as there have been manned airplanes fighting in combat, unmanned variations have also been present, albeit in more infantile stages of development and use. The distinction here is important: for all the potential and advantages of the manned aircraft, unmanned variants stood to deliver similar benefits without a corresponding risk to the pilot. The limitations of technology, however, would ultimately make unmanned platforms less appealing when compared to more capable manned platforms.

As RPAs developed over time, theories about how to use them advanced in parallel. Technological limitations, however, would keep these theoretical uses from materializing. Said otherwise, RPAs required a maturation period before they were capable of meeting expectations. In this regard, they reflected the same growing pains of air power, writ large. Air power critics often complained of over-promising and under-delivering, though time ultimately reveals evidence for a worthy rebuttal to the argument. With RPAs, many of the same vexing themes of air power development persisted: theory rarely became reality.

Once capable of becoming reality, RPAs found use in many of the same applications posited by original air power theorists. Historically, RPAs were scaled-down or actual versions of production-scale aircraft, modified for use without an onboard aircrew or pilot. Now, technology is advancing at such a pace as to afford much smaller platforms with the same, or even superior, payload, range, and loiter time of full-sized aircraft. As this trend continues, smaller RPAs successfully incorporate ISR capabilities that provide for intelligence-gathering without the consequential need for a dedicated runway. Air operations require specialized locations, criteria which make their locations limited and predictable. Small-scale RPAs potentially avoid these requirements and continually advancing technology implies they will be capable of delivering tactical effects similar to full-size aircraft without the infrastructure required by manned aircraft. In short, this new capability blends mobility and increased access in ways that could prove detrimental to US interests abroad.

Through technological advancements, platforms grew in capability while decreasing in size. The affordability, capability, and growing lethality of RPAs began to steadily increase even as their size decreased. By making lethality available at such small

costs and without considerable logistics-support requirements, small-scale RPAs became an effective tool for precision standoff attacks. There is an alarming ease to which adversaries can use open-market, commercial options to build and deploy small-scale RPAs as precision standoff weapons. Commercial market growth creates a demand for the use of small-scale RPAs for military and civil applications, which in turn, leads to increased technology that provides enhanced RPA capability at a decreased cost. Further, as capability and affordability advance, ease of use increases. These factors combine to provide an effective and affordable precision standoff weapon that is now available on the open market. With this capability, attacks against the military and civilian infrastructure of the US and its allies become more feasible and likely.

Thesis Scoping and Theory

The author recognizes the ongoing dialogue concerning platform terms and acronyms, such as Unmanned Aerial Vehicle (UAV) and System, Unmanned Combat Air Vehicles, RPAs, and the more ominous "drone." The Federal Aviation Administration (FAA) refers to UAVs as devices used, or intended to be used, for flight in the air without an onboard pilot.[5] While the use of drone and UAV remain popular in the contemporary vernacular, this thesis adheres to current US Air Force doctrine and uses RPA to describe the platforms herein.[6] This thesis builds upon the FAA definition considerably and defines RPAs as aerial vehicles that do not carry a pilot or human operator on board, use aerodynamic properties to create lift and sustain flight, fly autonomously or by remote (manned) mechanisms, and can ferry a payload.[7] The "small-scale" qualifier specifically refers to a class of unmanned aircraft weighing 55 pounds or less which fly at 400 feet elevation and below.

---

[5] Nick Sabatini, Federal Aviation Administration, "Federal Register: Unmanned Aircraft Operations in the National Airspace System, Docket No. Faa-2006-25714," February 6, 2007, accessed April 17, 2014, http://www.gpo.gov/fdsys/pkg/FR-2007-02-13/html/E7-2402.htm.

[6] Other terms may be used in quotations or direct references. For example, a magazine headline may refer to UAV or drone, which will remain as printed for this paper. For the purpose of this body of work, RPA is interchangeable unless otherwise specified.

[7] This definition borrows from Eugene Miasnikov in his 2005 report. See Eugene Miasnikov "Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects", *Center for Arms Control, Energy and Environmental Studies, Moscow Institute of Physics and Technology* (2005): 6.

This category adheres to commonly accepted categorization amongst RPA enthusiasts, experts, and the guidelines set by the FAA in delineating airspace restrictions by platform. The FAA distinction is particularly important as the elevation and weight threshold identifies the hobbyist market of remote-controlled aircraft, upon which this thesis leans heavily in theory. Small-scale RPAs find close relatives in the family of commercially available hobby aircraft, providing cost-effective substitutes to purpose-built military RPAs. This represents a conceivable gateway from malicious intent to execution of a terrorist attack by turning small-scale RPAs and hobby aircraft into precision airborne improvised explosive devices. David Mets eloquently summarizes this theme: "One way of looking at the history of military development is seeing it as an eternal search for standoff and precision to discover what one's enemy might be doing, or to strike him blows with minimum risk to one's health."[8]

Overall, this thesis postulates that small-scale RPAs weighing less than 55 pounds represent a specific weapons demographic capable of executing low-cost, high-return attacks against an air base through disruption and harassment of U.S. operations. Airpower often requires an in-theater footprint, and the proper selection and sustainment of an air base enhances air power and power projection. By conducting offensive operations, however, the air base will inherit a level of vulnerability. This vulnerability is a valid concern; history demonstrates that in ten different conflicts from 1940 to 2013, air bases suffered hundreds of attacks by myriad methods. (e.g. glider, airborne, air assault, standoff weapons, and vehicular or foot penetrations)

If the historical trend is an indicator, then standoff threats will prove particularly daunting, and precision weapons will exacerbate the problem.[9] Instead of highly organized mass attacks seeking to create strategic events or gain strategic advantage, adversaries will harass and interrupt air base operations as a low-cost, compelling option to blunt US air power. This is largely because the centrality of airpower to modern

[8] David Mets, "Rpas: Revolution or Retrogression", *Air Force Research Institute Papers* (paper 2010-1, April 2010): 1-25. Here, Mets quotes Ames R. Reinhardt et al., "Future Employment of UAVs: Issues of Jointness," *Joint Forces Quarterly*, Summer 1999, 36.
[9] Alan Vick, *Snakes in the Eagle's Nest: A History of Ground Attacks on Air Bases*, Project Air Force (Santa Monica, CA: RAND, 1995), xxi.

warfare makes the airfield an increasingly alluring target.[10] Defending against these attacks requires security measures which may inconvenience the normal functioning of an airfield; large attacks are not required to effectively harass an airfield as small attacks have proven quite effective.

The US Air Force remains successful in establishing air superiority and preventing enemy *air* attacks against US ground positions, despite a prevalent threat to the air bases from which air power derives. The Air Force is not successful, however, at eliminating *standoff* attacks that threaten to erode air power by attacks on the air base. Before it was superseded, Air Force Instruction (AFI) 31-301, *Air Base Defense*, recognized the danger of standoff weapons, saying that standoff attacks are, "the most likely threat to Air Force personnel and resources."[11] Defending against these attacks is increasingly difficult and requires command of multiple square miles of terrain outside the air base. In many cases, this area includes civilian cities that are incredibly difficult to police without dedicating vast (and often scarce) resources, potentially granting sanctuary for a threat to the air base and its aircraft.

Although aircraft remain extremely lethal in the air, they represent a lucrative and vulnerable target on the ground.[12] Technologically advanced aircraft are very susceptible to attack and can suffer incapacitating damage from a few well-placed rounds of ammunition or small amounts of explosive material.[13] While part of air base defense includes hardened aircraft shelters, dispersal of assets and infrastructure reinforcements, these methods are passive defenses that do little to prevent standoff attacks. At best, these measures alter the risk-reward calculations of the enemy, making air assets more difficult to target and attack, thus increasing risk to an unacceptable level. As technology increases and offers greater range and precision to the enemy, it will make standoff attacks easier and potentially adjust the risk to more acceptable levels for the adversary.

Air superiority remains an extension of the air power projection capability afforded by an air base. Without adequate protection, an air base's effectiveness will erode as

---

[10] Vick, *Snakes in the Eagle's Nest*, 4.
[11] Sagraves, "Air Base Defense," 35, quoting Air Force Instruction (AFI) 31-301, *Air Base Defense*, 15 May 2002, 6. AFI31-301 was later superseded by AFPD 31-1, *Integrated Defense*
[12] Glenn. Palmer, "Air Base Security Operations: An Air Component Responsibility," School of Advanced Air and Space Studies, 2006, 44.
[13] Palmer, "Air Base Security Operations," 1.

critical resources are devoted to security and defense versus offensive operations that bridge sortie support to air superiority. Though attacks pose a direct threat to air base security, doctrine and policy risk posing a proxy threat by creating battlefield conditions that may exacerbate the risk of enemy standoff attacks.

Doctrinal changes altered the strategy for air base defense and its allocation of resources due to changes in battlefield composition; contiguous lines of operation rarely exist any longer, and the more commonly seen ink-blot disposition of forces means a dispersal of ground support may not directly support the air base. Given that the air base remains highly vulnerable to standoff attack, these doctrinal changes mean the methods and resources used to protect the air base will more likely be an Air Force obligation. As such, the Air Force must determine the optimal means of defeating the enemy outside the perimeter, in the critical terrain used for standoff attacks.[14]

Bureaucratic challenges in US and international policy exacerbate the threat and increase the ease with which these platforms can be used maliciously. If small-scale RPAs pass from theory into a realistic method of attack, their success depends on the following factors: capability (e.g. platform and payload; communication and navigation of the actors), intent, and physical defense against the attack. Other factors complicate prevention and contribute to the threat, such as market growth signaling a rise in popularity of unmanned vehicles that make an attack attractive, and policy challenges that offer loopholes by which an attack might be mounted. The US must act decisively and intelligently if it is to exploit a technological advancement for its own good while simultaneously denying such privilege to the enemy.

[14] Palmer, "Air Base Security Operations," 35.

Chapter 2

WHY AN AIR BASE?

Introduction

Overall, this thesis postulates that small-scale RPAs weighing less than 55 pounds represent a threat capable of executing low-cost, high-return attacks against an air base through disruption and harassment of U.S. operations. The intent of this chapter is to further dissect that argument and first introduce the nature and necessity of air bases for the projection of air power, as well as the corresponding risk an air base faces from willing and capable enemies. Specifically, air power often requires an in-theater footprint, and the proper selection and sustainment of an air base enhances air power and power projection. By conducting offensive operations, however, the air base will inherit a level of vulnerability. This vulnerability is a valid concern; history demonstrates that in ten different conflicts from 1940 to 2013, air bases suffered hundreds of attacks by myriad methods. (e.g. glider, airborne, air assault, standoff weapons, vehicle and foot penetrations, etc.)

If the historical trend is an indicator, then standoff threats will prove particularly daunting, and precision weapons will exacerbate the problem.

[1] Instead of highly organized mass attacks seeking to create strategic events or gain strategic advantage, adversaries will harass and interrupt air base operations as a low-cost, compelling option to blunt US air power. This is largely because the centrality of airpower to modern warfare makes the airfield an increasingly alluring target.[2] Defending against these attacks requires security measures which may inconvenience the normal functioning of an airfield; large attacks are not required to effectively harass an airfield, and small attacks have proven quite effective. Bearing these facts in mind, leadership can assess strategies for defense.[3]

---

[1] Alan Vick, *Snakes in the Eagle's Nest: A History of Ground Attacks on Air Bases*, Project Air Force (Santa Monica, CA: RAND, 1995), xxi.
[2] Vick, *Snakes in the Eagle's Nest*, 4.
[3] Vick, *Snakes in the Eagle's Nest*, 101, 107.

Why an Air Base?

Not long after the Wright Brothers' first flight in 1917, military applications for air power took shape. Yet over-promising and under-delivering often characterized the early days of air power theory; a "say-do" gap existed between the theoretical potential of the aircraft and the real-world results of its application. This was the case throughout World War I, during the combined bomber offensive in World War II, as well as the Linebacker campaigns of Vietnam. Air power eventually revealed itself in the Cold War era as a reliable instrument to support national security, but the growing pains of its maturation left lingering doubts from its critics. However awkward its development and however vocal its critics, air power's message remained consistent: if used correctly, it would offer an incredible advantage over an enemy, even more so if the adversary lacked air forces of its own.

Early air power theorists sought to blunt an adversary's combat effectiveness through an effective use of air power, specifically against aircraft on the ground. Giulio Douhet said, "It is easier and more effective to destroy the enemy's aerial power by destroying his nests and eggs on the ground than to hunt his flying birds in the air."[4] Douhet's maxim has a careful distinction, in that destroying the eggs on the ground does not strictly dictate using ground forces in the attack. Quite the contrary, the advantage of an aircraft is its ability to strike above and beyond an adversary's reach, and using air assets for an attack can yield decisive effects on the ground. Aircraft remain an excellent tool for this endeavor and provide a menu of options for a strategist.

Ultimately, the lethal capabilities of an aircraft must originate from the nest. Although the aircraft remains the nexus between air power theory and air power effectiveness, the aircraft and its subsequent lethality originate from Douhet's nest. To this end, the air base remains central to the projection of air power and symbolizes a valuable target for enemy attacks. An air base derives its power from multiple factors, including: opportunity; location; geography and topography; and politics.[5]

---

[4] Giulio Douhet, *The Command of the Air* (Washington, DC: Office of Air Force history, 1982 [originally published in 1921], 53-54.

[5] Frederick Shaw, *Locating Air Force Base Sites: History's Legacy* (Washington, DC: Air Force History and Museums Program, 2004) 1-8.

First, an air base represents a powerful tool in the projection of power, both economically and in terms of its value to the mission. Traditional CONUS and OCONUS locations employ thousands of people; and, even in an expeditionary environment where the local population may be disparate and isolated, an air base offers economic benefit. In each case, there is a direct tie to job security and economic vitality.[6] Further, the more capable an air base, the greater its contribution to the overall projection of air power and, by extension, the sense of value it provides to the mission.[7] To professional airmen, the ability of an air base to project power may directly provide a valuable sense of contribution, validate their cause, and foster morale essential to combat operations.

On the contrary, an air base also represents a competitor. Economic stability may embody the capitalist or free market nature loathed by an adversary, especially in an irregular war that seeks to manipulate populations, versus seizing and holding territory. Furthermore, air bases are industrial facilities prone to noise and chemical pollution and may pose a safety concern.[8] An aircraft accident injuring nearby residents or causing damage to local towns is a potent propaganda tool for anti-US sentiment. Ultimately, air base operations may continually remind the enemy of – and increase frustration over – a foregin presence. To this end, air bases remain valuable targets worthy of dedicated attention by enemy forces.

Second, the location of an air base is pivotal to the effective projection of air power. The USAF currently possesses the ability to conduct long-range, worldwide strikes from positions originating within the US. (e.g., B-2 strikes originating in the US, bombing targets in Afghanistan, then returning to the US in a single sortie; ICBMs, offensive cyber attacks, etc.) However, these are exceptions to the conventional rule of an air base residing within the theater of operations and serving to project combat air power in relative proximity to the fight. Proximity as a strategy is not a new consideration; in 1925, Orville Wright testified before the Morrow Board, speaking on the importance of

[6] Shaw, *Locating Air Force Base Sites,* 1.
[7] Shaw, *Locating Air Force Base Sites,* 1.
[8] Shaw, *Locating Air Force Base Sites,* 1.

suitable airfields for the effective basing and operating of air forces.[9] To this end, location of an air base with regard to power projection has always been a vital concern.[10]

Third, the geography and topography of the area surrounding an air base is a vital consideration. For example, in the pioneering days of aviation from 1907-1917, technological limitations on the aircraft meant the surrounding geography and topography demonstrated favorable weather and an agreeable climate.[11] Prevailing winds were important during the times of turf runways since crosswinds could wreak havoc on smaller, lighter aircraft.[12] Additionally, an airfield had to possess certain physical features such as being level, easy to repair, and capable of shedding and draining water quickly.[13] After WWI, aircraft technical limitations affected site selection – the main portion of the base formed the center of an aircraft's radius of flight. For defensive purposes, bases were located near the center of the region where an aircraft operated or near the target an aircraft was assigned to protect.[14]

This doctrine remains only partially in effect today, as modern airframes routinely endure the crosswinds that were once so detrimental and the effective range of today's platforms helps sever the bond between a base and the resident aircraft's radius of flight. An air base in 1917 required adequate transportation, utilities, housing, and base support and recreation facilities; the same factors remain important today. Further, after WWI, proximity to major centers of technical expertise was important.[15] Today's Air Force shares this concern, though expeditionary operations may lack robust technical and engineering support due to austere locations and paucity of available resources. Lastly, from the earliest days of flight until now, the relative size of a base increased as aircraft

[9] Shaw, *Locating Air Force Base Sites*, 5. In 1925, President Coolidge created the Morrow Board, led by Dwight Morrow, the banking executive and future father-in-law to Charles Lindbergh. President Coolidge tasked the board to recommend policy for national aviation and the future of US airmail components. The board provided several recommendations, including non-military civil aviation standards to be set by the government. For more, see Smithsonian National Postal Museum at http://www.postalmuseum.si.edu/airmail/airmail/public/airmail_public_postal_long.html. (Accessed 17 Feb 2014)
[10] Shaw, *Locating Air Force Base Sites*, 5.
[11] Shaw, *Locating Air Force Base Sites*, 6.
[12] Shaw, *Locating Air Force Base Sites*, 7.
[13] Shaw, *Locating Air Force Base Sites*, 7.
[14] Shaw, *Locating Air Force Base Sites*, 6.
[15] Shaw, *Locating Air Force Base Sites*, 6.

became larger, faster and heavier.[16] Early airfields survived with as few as ten acres, but by 1940 the Army Air Corps sought areas with thousands of acres capable of accommodating hardened runways and increasing infrastructure such as housing, recreation, maintenance, and other aviation support.[17]

Fourth and finally, the bureaucratic and political considerations of air base selection remain increasingly important. Though air base acreage remained primarily a topographical or geographical concern in the past, it carries significant political ramifications then and now. The larger an airbase and the more technologically advanced the aircraft assigned to it, the more upkeep and maintenance required for aviation support. This translates into job creation and economic vitality (as previously mentioned), which catches considerable political attention. In the past, the issues of politics, economics, and local support proved too tightly intertwined to be neatly separated.[18] Contemporary and future operations should not expect to escape the same scrutiny.

Although today's power projection can take place from virtually anywhere on the globe, doing so carries a degree of strategic and physical cost. There is an undeniable benefit to securing a standoff distance; however, an excessive distance may trade security for combat capability. Generally speaking, it is cheaper and more accommodating to launch from bases close to the target, understanding that proximity may breed risk.

In conclusion, while the nexus between air power theory and air power execution is the aircraft, the air base provides the critical infrastructure and support that makes the aircraft inseparable from power projection. Said otherwise, the lethal capabilities of an aircraft originate from the nest. Air bases remain a mighty and formidable tool in power projection but their site selection and method of operation rely on distinct, significant factors: opportunity; location; geography and topography; and politics. Air power and power projection come from the air base just as much as the aircraft. For these reasons, the air base remains central to the projection of air power and symbolizes a valuable target for enemy attacks. The following section elaborates on this threat.

[16] Shaw, *Locating Air Force Base Sites*, 7.
[17] Shaw, *Locating Air Force Base Sites*, 7.
[18] Shaw, *Locating Air Force Base Sites*, 7.

A Short History of Air Base Vulnerability

Early on the morning of 14 June 1951, enemy pilots climbed aboard two Polikarpov PO-2 aircraft and departed Sariwon Airfield, North Korea, making a low and slow southbound flight toward Seoul and unsuspecting United Nations forces. Constructed of wood and covered in canvas, the open cockpit, single-engine bi-planes produced a diminutive radar signature, appearing as two slow-moving "blips" emerging amongst the ground clutter for radar operators of the 606th Aircraft Control and Warning Squadron. Several minutes later, at approximately 0315 hours, the first of the formation flew to striking range of the ground forces at Suwon Airfield, dropped two bombs on the airfield, and narrowly missed the squad of engineers repairing the runway. The second aircraft continued to Inchon, dropping its bombs on an Eighth Army motor park. Both aircraft then turned northward and made a safe escape.[19]

On the evening of 15/16 June 1951, a Blochavidan MBE-2 pusher-engine seaplane conducted an unsuccessful strafe of Kimpo airfield, accomplishing little more than a near miss on a jeep carrying policemen. On the next night, however, a separate flight of two PO-2s dropped a pair of small bombs over Suwon airfield with much greater success. The first bomb caused damage to equipment inside the 802d Engineer Aviation Battalion's motor pool, while the second bomb scored a direct hit, destroying an F-86 Sabre and damaging eight others, four of them seriously. In this instance, a small, cloth-winged bi-plane executed a well-timed blow against far superior jet aircraft on the ground – a location where they were, and remain, the most vulnerable. This singular attack did more damage against the Sabres than had all combat with MiGs up to this time.[20]

If these attacks were hard to oppose in 1951, they proved equally annoying in 1952 when after nearly a year's respite, North Korean pilots resumed this type of harassment attack.[21] Often, enemy raids escaped harm from United Nations forces who were unable to target them from anti-aircraft artillery on the ground or from air-to-air engagements as UN jets were often incapable of matching the 80-knot airspeed of propeller bi-planes. Additional attacks ensued, utilizing the same tactics and platforms. On 13 October 1952,

[19] Robert F. Futrell, *The United States Air Force in Korea, 1950-1953*, (Washington, D.C.: Center for Air Force History, 1983), 309.
[20] Futrell, *The United States Air Force in Korea*, 309.
[21] Futrell, *The United States Air Force in Korea*, 662.

four PO-2 aircraft bombed and strafed radar installations on Cho-do Island, killing five Korean civilians and wounding two Americans.[22] Subsequent raids took place on 26 November, 5 December, 10 December and 30 December, though some of the enemy aircraft succumbed to successful Skynight and Corsair engagements. Attacks resumed during the night of 15 April 1953 when several enemy aircraft attacked Cho-do, destroying an artillery weapon and killing two artillerymen. United Nations forces grew tired of these attacks, but found the aircraft to be an elusive threat against their air defense platforms.

As the war continued, North Korean pilots utilized PO-2, LA-11 and Yak-18 aircraft to increase the attack frequency and target high-value assets. Enemy raids successfully bombed Seoul from 15-17 June 1953, including the mansion of President Syngman Rhee and Seoul infrastructure, proving that national-level targets remained susceptible. On the night of 16/17 June 1953, approximately 15 of these aircraft set off several fires and a subsequent blaze at Inchon which destroyed five million gallons of fuel. Subsequent raids were intercepted, and the last sortie destroyed on 16 July 1953.

Characterized by their late-night arrivals, these attacks came to be known by UN forces as "Bedcheck Charlies."[23] Although they rarely caused significant strategic damage, they still represented a "small but very antagonizing thorn in the side" of the United Nations Force."[24] Bedcheck Charlie flights were periodically successful in causing damage to UN forces and equipment, but rarely amounted to more than a harassing tactic or heckling raid. On a larger scale, Bedcheck Charlie crews demonstrated a troubling ability to penetrate an air defense system, showing that no defense is perfect and cementing among UN forces the need for dispersed air facilities and a passive defense.[25] Robert Futrell elaborates, "Since the standard jet interceptors were not able to cope with prop-driven planes, FEAF (Far East Air Forces) thought that antiaircraft artillery should have been the principal defense against low- and slow-flying hostile aircraft, at least until all-weather interceptors received moving target interceptor

[22] Futrell, *The United States Air Force in Korea*, 662-3.
[23] Futrell, *The United States Air Force in Korea*, 310.
[24] Futrell, *The United States Air Force in Korea*, 310.
[25] Futrell, *The United States Air Force in Korea*, 665.

radar."[26] Despite the tremendous advancements in radar and defense systems since the 1950s, the lingering significance of Bedcheck Charlies is not their tactic, so much as it is what they represent: a bookmark for historians, representing the last attacks against American ground forces by enemy air forces.[27]

History consistently reveals that an attack upon an air base is a clear and present danger during a conflict, especially in contemporary operations where the enemy seeks to blunt the effectiveness of air power by irregular or asymmetric means.[28] Enemies are wise to target aircraft on the ground with everything they have; to engage the U.S. military head-to-head in a conventional fight is a foolhardy gesture for a non-state actor lacking sufficiently more robust forces. As a result, these actors fight *as they can*, mostly through irregular means aimed not necessarily at defeating enemies, but delaying or disrupting them using standoff tactics. (figure 1)

[26] Futrell, *The United States Air Force in Korea*, 665.

[27] This claim is often made in air power circles, to include an address by General John P. Jumper in his speech to the National Logistics Officers Association Conference in Phoenix, AZ in 2000. Opponents of the claim cite the attack of Lima Site (LS) 85 in Vietnam, 12 Jan 1968, when AN-2 Colt aircraft attacked the then-classified TACAN location by rocketing, strafing and dropping modified Russian mortar rounds as improvised bombs. It is possible that the Lima Site 85 reference remained in the shadows of classified history for many years, allowing the unclassified history of Bedcheck Charlies to prevail as the last attack from an enemy air force. The intent of this citation is not to determine the historical mantle upon which this fact ultimately resides, but to highlight (as a result of air superiority) the rarity of enemy air forces attacking US ground positions. For more on LS-85, see https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/95unclass/Linder.html (accessed 17 Feb 2014) and Timothy Castle, *One Day too Long: TOP SECRET Site 85 and the Bombing of North Vietnam* (New York, NY: Columbia University Press, 1999), p. 2

[28] Robert D. Sagraves, "Airbase Defense Outside the Wire: Air Support for Defending Expeditionary Air Bases on the Nonlinear Battlefield," Maxwell AFB, AL (2006), 4.

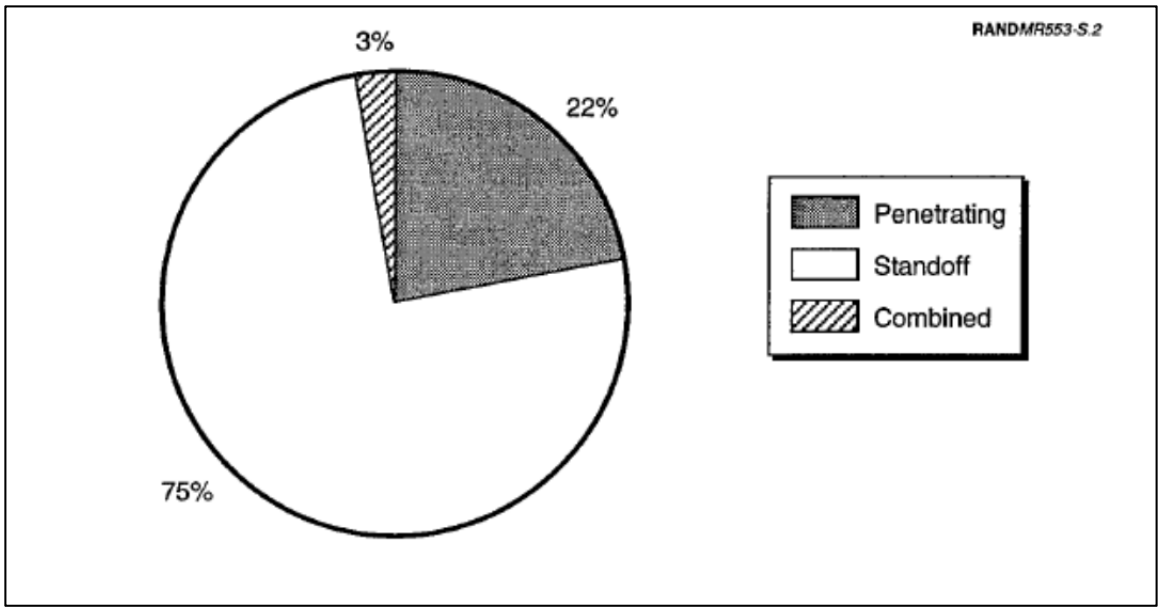

Figure 1. Air Base Attack Tactics, 1940-1992
Source: Alan Vick, "Snakes in the Eagle's Nest," p. xvii

This is what many of the world's armies have done through history, attacking air bases at least 645 times over the course of ten conflicts from 1940-1992.[29] These attacks (from the hands of airborne, airmobile, infantry, and armor elements) damaged or destroyed more than 2,000 aircraft. Although most of the attacks came from conventional forces employing conventional methods (parachute, glider, amphibious landings, helicopter insertions, etc.), terrorist and guerilla operations constitute a portion of the totals.[30]

Between 1940 and 1992, attacks on air bases encompassed four distinct categories: capture airfield, deny use, harass defender, and destroy aircraft.[31] (figure 2) These attacks rarely sought to capture the airfield and use it as a staging location or airhead, but more frequently sought to destroy aircraft and equipment. Of the 645 attacks identified across these categories, only six percent constituted an attempt at airfield seizure. Most of those occurred in World War II, although U.S. forces overtook and used airfields in

[29] Vick, *Snakes in the Eagle's Nest*, 13. Vick claims, "This number is based on *deliberate* attacks on airfields, whether they were independent operations or part of a larger offensive. It does not include the many times that ground forces overran airfields on their way to other objectives." [emphasis in original]
[30] David A. Shlapak and Alan Vick, *Check Six Begins on the Ground: Responding to the Evolving Ground Threat to US Air Force Bases*, Project Air Force (Santa Monica, CA: RAND, 1995) 21-22.
[31] Vick, *Snakes in the Eagle's Nest*, figure S-1, xvii.

Panama (1989) and Grenada (1983), while Soviet forces took Afghan airfields (1979).[32] The destruction of aircraft and equipment accounted for 384 separate attacks, constituting 60 percent of the overall total.[33]

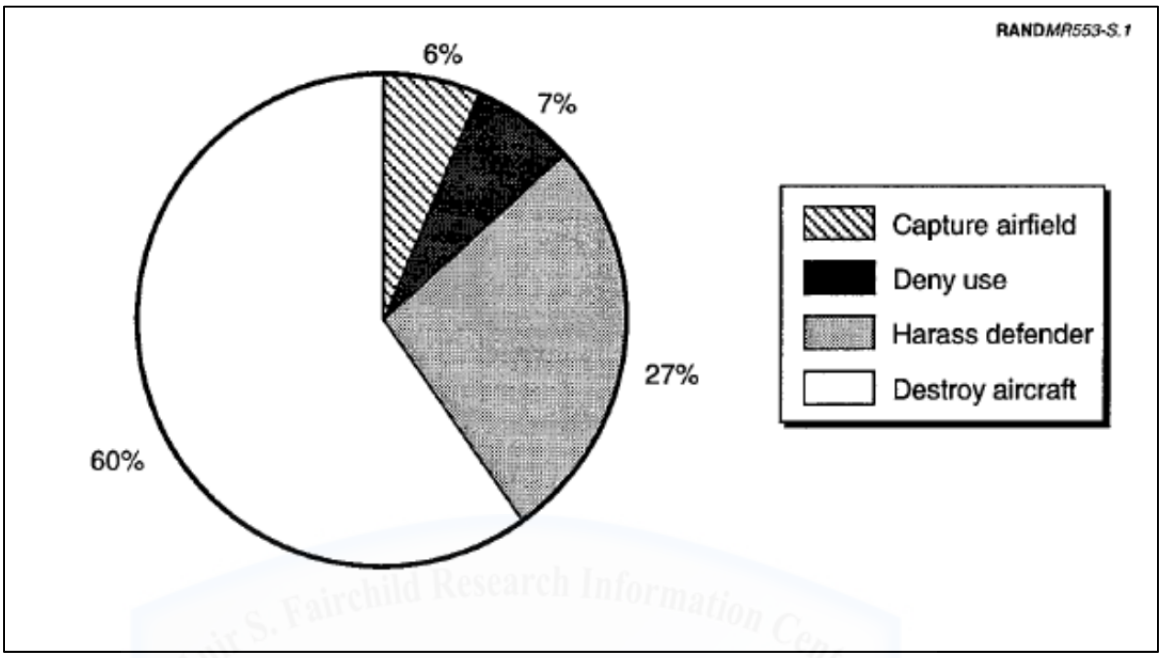

Figure 2. Airfield-Attack Objectives
Source: Alan Vick, "Snakes in the Eagle's Nest," p. xvii

The timeframe for these statistics ended over a decade ago; however, the wars in Iraq and Afghanistan saw multiple attacks upon U.S. and coalition air bases, indicating the historical trend continued. For example, U.S. air bases in Iraq during Operation IRAQI FREEDOM (OIF) endured over 1,000 attacks in just two years.[34] A separate source claims that during OIF and Operation ENDURING FREEDOM (OEF), the enemy used standoff weapons in over 1,500 attacks against US airbases with 400 of them taking place in one year against Balad AB, Iraq alone. In these attacks 39 personnel were killed or injured and five aircraft sustained damage.[35] The specific details of these attacks remain

[32] Vick, *Snakes in the Eagle's Nest*, xvi.
[33] Vick, *Snakes in the Eagle's Nest*, xvi.
[34] Ron Gray, "Integrated Swarming Operations for Air Base Defense: Applications in Irregular Warfare," Naval Postgraduate School, 2006, p. 11. Gray is quoting Brigadier General Robert Holmes, former Director of Air Force Security Forces (A/7S), "Security Transformation" brief to the Air Force CORONA Conference, December 2004.
[35] Glenn Palmer, "Air Base Security Operations: An Air Component Responsibility," School of Advanced Air and Sapce Studies, June 2006, 35, 48. Palmer is also quoting Brigadier General Holmes, here from

classified by United States Air Forces Central Command (USAFCENT), however the damage inflicted did not prevent the Air Force from accomplishing a mission of projecting air power.[36] These attacks imply that current air base defense doctrine is ineffective in deterring, detecting, delaying, and denying enemy attacks against expeditionary outposts. This is especially true for those attacks originating outside the base perimeter.[37] The consequent difficulty in finding, targeting and eliminating threats originating in an urban environment may restrain air power's effectiveness and leave the base with a possibly indefensible position against standoff attacks.

Due to a historical precedent of air base attacks, as well as a known deficiency in perimeter security, establishing the proper security posture to defend the air base and its assets remains paramount in expeditionary operations, especially against an adversary using irregular warfare tactics. This risk is elevated when Army operations do not establish a secure area for air operations, or do not apportion assets for air base defense. (discussed in greater depth in Chapter 3) Given these considerations, leadership should continue exercising diligence with regard to force protection and air base defense during expeditionary operations.

As previously mentioned, it is expected that gaining and maintaining air superiority in expeditionary operations requires in-theater fixed-wing assets. Forces stationed outside the theater enable air power; however proximity offers flexibility, and long-term operations eventually call for an in-theater presence. Due to security concerns, these high-value assets primarily operate from a safe quarter, close enough to execute ISR, mobility, or strike operations, yet removed from immediate hostilities to the best extent practical. Those assets closest to hostilities require enhanced protection and defense against attack.

Robert Sagraves claims, "Having demonstrated its aerial supremacy in every major conflict since Operation Desert Storm, the US will be challenged by future adversaries who will increasingly seek asymmetrical ground-based means to blunt US air power."[38]

"Air Base Security Operations: The Importance of Security Operations and an Organizational Construct to Protect and Project Air Power duering Expeditionary Warfare" (White Paper, HQ USAF, n.d.), 3.

[36] Palmer, "Air Base Security Operations: An Air Component Responsibility," 52.

[37] Palmer, "Air Base Security Operations," 11. Gray's requests for unclassified data were denied and not releasable for his thesis.

[38] Sagraves, "Airbase Defense Outside the Wire," 4.

Although Sagraves' claim was made in 2006, present-day operations confirm the longevity of his statement; the U.S. faced asymmetrical ground threats until its withdrawal from Iraq and remains challenged by an asymmetrical enemy on the ground in Afghanistan. It is not surprising or revealing that air power has done much for warfare in the preceding decades, nor is the expectation that an enemy will seek to minimize the advantage air power brings. Employing irregular warfare techniques provides an adversary with cost-effective means to fight a larger, more powerful enemy without undue risk to its own forces. These hit-and-run tactics utilize speed, mobility and lethality in a small footprint, avoiding the massing of forces that an adversary can easily target.

Lawrence of Arabia articulated the benefits of such tactics in his 1920 work, "The Evolution of a Revolt." In it, he emphasized the need to preserve resources in an attack, never trying to improve or maintain an advantage. Rather it was preferred to move off and strike again at another target. These attacks are tip-and-run – not pushes, but strokes. Additionally he warns against needlessly consolidating your own resources, stating that in an irregular war, if two men are together, one is being wasted. To Lawrence, victory in an irregular war depended on the just use of victory, speed and concealment.[39] This preservation of resources, tip-and-run tactics, speed and concealment appear to be the traits of standoff attacks used by the enemy in Afghanistan.

An enemy employing these tactics is difficult to counter and therefore raises questions for the role of U.S. air power in a limited or irregular war. Roger Trinquier doubted the effectiveness of air power in a limited (specifically, guerilla) war. Specifically, air attacks offer secret preparation and rapid execution but can only be decisive if they are massive, plus this expends considerable resources. Additionally, surprise comes only with the first bombardments, then the enemy quickly disperses and seeks concealment or camouflage. At this point, subsequent attacks are less profitable, and future targeting is far more difficult.[40]

Preserving this argument for contemporary conflicts questions the ability of an air power to provide adequate air base defense in an irregular war. Perhaps this is less an

[39] TE Lawrence, "The Evolution of a Revolt," US Army Command and General Staff College (Ft Leavenworth, KS: Combat Studies Institute, originally printed 1920) 20.
[40] Trinquier, "Modern Warfare," 80.

issue of physical capability but is more a concern of targeting in urban environments where the enemy blends with the population. There are certainly platforms capable of bolstering perimeter and air base defense (e.g., AC-130, A-10, AH-64), however employing these against an elusive enemy finding sanctuary in the surrounding population is problematic. Additionally, permanently dedicating these platforms to defend the air base may remove them from other operational requirements, such as directly supporting forces in the field. Commanders must decide between security of the base or security of the forces engaging the enemy; the availability of small-scale RPA platforms will influence their decision making. During the initial stages of the conflict when hostilities are greatest, defending the air base may be the most prudent. Once a secure perimeter and standoff footprint is established, it may be more appropriate to transition these aircraft to offensive operations.

The location of an air base matters greatly in conducting air power operations. Choosing a location depends on multiple variables, not the least of which are status of facilities, prevailing weather patterns, accessibility of logistics and base support and the ability to conduct operations. Understanding or predicting the adverse impact of an air base location is less simple. In the remote, unprotected areas likely to house forward operating bases (FOBs), bedding down aircraft is impractical. Not only would doing so require a robust infrastructure for sortie generation and power projection, but any permanently assigned aircraft would provide a lucrative target for the enemy.

If a main operating base is highly susceptible to enemy provocation and standoff attacks, FOBs are at least as prone to attack due to a less robust defensive posture. Without dedicated aircraft for close air support and perimeter defense, FOBs require on-call air defense assets and potentially offer a softer target than an established main operating base and its subsequent defense mechanisms.[41] As a corollary, lacking these assets may devalue the outpost to an adversary seeking more valuable targets. This poses a theoretical risk-reward for standoff attacks: the FOB offers a greater ease of attack but less payoff in terms of damage inflicted. Ideally, aircraft use time and space to gain

[41] More specific data on FOB attacks remains classified and may require several years to reveal the finer details.

distance that guards against enemy reach, yet remain close enough for rapid strike requirements.

Conclusion

The projection of air power rests upon the nature and necessity of air bases. Although the aircraft remains the nexus between air power theory and air power effectiveness, the aircraft and its subsequent lethality originate from Douhet's nest. To this end, the air base remains central to the projection of air power and symbolizes a valuable target for enemy attacks. History reveals nearly 2,000 known attacks against air bases from 1940 until today, suggesting that an air base, so long as it supports air power and power projection, faces a legitimate risk of attack. Though the effectiveness of these attacks will vary, there remains a consistent theme of harassment and interruption versus destruction or seizing. Weakened perimeter defenses or alluring targets inside the perimeter pose compelling reasons for an enemy to risk standoff attacks. As technology increases, so will the ability to execute these attacks with precision. Currently, and despite these challenges, the Air Force remains successful in maintaining air superiority and preventing enemy air attacks against US ground positions. The question then becomes, Can the Air Force guarantee this claim into the future? The next chapter discusses competing service doctrine which may undermine such a pledge.

Chapter 3

DOCTRINE AND AIR BASE DEFENSE

Introduction

As previously highlighted, the US Air Force remains successful in establishing air superiority and preventing enemy *air* attacks against US ground positions, despite a prevalent threat to the air bases from which air power derives. The Air Force is not successful, however, at eliminating *standoff* attacks that threaten to erode air power by attacks on the air base. Before it was superseded, Air Force Instruction (AFI) 31-301, *Air Base Defense*, recognized the danger of standoff weapons, saying that standoff attacks are, "the most likely threat to Air Force personnel and resources."[1] Defending against these attacks is increasingly difficult and requires command of multiple square miles of terrain outside the air base. In many cases, this area includes cities that are incredibly difficult to police without dedicating vast (and often scarce) resources, potentially granting sanctuary for a threat to the air base and its aircraft.

Although aircraft remain extremely lethal in the air, they remain a lucrative and vulnerable target on the ground.[2] Technologically advanced aircraft remain susceptible to attack and can suffer incapacitating damage from a few well-placed rounds of ammunition or small amounts of explosive material.[3] While part of air base defense includes hardened aircraft shelters, dispersal of assets, and infrastructure reinforcements, these methods are passive defenses that do little to prevent standoff attacks. At best, these measures alter the risk-reward calculations of the enemy, making air assets more difficult to target and attack, thus increasing risk to an unacceptable level. As technology increases and offers greater range and precision to the enemy, it will make standoff attacks easier and potentially lower the risk to acceptable levels.

Ultimately, history reveals that standoff threats are the most likely mechanism to undermine air-base effectiveness. This is the product of most opponents lacking the

---

[1] Sagraves, "Air Base Defense," 35, quoting Air Force Instruction (AFI) 31-301, *Air Base Defense*, 15 May 2002, 6. AFI31-301 was later superseded by AFPD 31-1, *Integrated Defense*

[2] Glenn. Palmer, "Air Base Security Operations: An Air Component Responsibility," School of Advanced Air and Space Studies, 2006, 44.

[3] Palmer, "Air Base Security Operations," 1.

capability, capacity, or technology to defeat the US Air Force in the air.[4] The most challenging threats are likely disruptive attacks in an irregular-warfare context.[5] The resulting disruptions potentially erode the Air Force's ability to gain and sustain the air superiority relied upon by joint, allied, and coalition forces.

Subsequently, air superiority remains an extension of the air power projection afforded by an air base. Without adequate protection, an air base's effectiveness will erode as critical resources are devoted to security and defense versus offensive operations that bridge sortie support to air superiority. Though attacks pose a direct threat to air base security, doctrine and policy risk posing a proxy threat by creating battlefield conditions that may exacerbate the risk of enemy standoff attacks.

US Army doctrine underwent significant changes resulting from the strain placed upon it by combat operations in Iraq and Afghanistan, though the post-Cold War character of conflict is also a consideration the Army factored in its doctrinal shifts. Part of this change included the abrogation of an agreement between the Army and the Air Force for air base defense. Additionally, Army doctrinal changes altered the perception of the battlefield and morphed from positional to functional elements, and from front and rear areas to contiguous and noncontiguous areas of operation controlled at the tactical level.

These doctrinal changes alter the strategy for air base defense and its allocation of resources due to changes in battlefield composition; contiguous lines of operation rarely exist any longer and the more commonly seen ink-blot disposition of forces means a dispersal of ground support that may not directly support the air base. Given that the air base remains highly vulnerable to standoff attack, these doctrinal changes mean that the methods and resources used to protect the air base will more likely be an Air Force obligation. As such, the Air Force must determine the optimal means of defeating the enemy outside the perimeter, in the critical terrain used for standoff attacks.[6]

[4] Palmer, "Air Base Security Operations," 1, and Dr. James Kiras (School of Advanced Air and Space Studies, Maxwell AFB, AL), interview by the author, 28 February 2014.
[5] Palmer, "Air Base Security Operations," 45.
[6] Palmer, "Air Base Security Operations," 35.

Changes in the Responsibility of Air Base Defense

Since its inception in 1947, the Air Force relied upon the Army for defending and protecting the air base so that the Air Force could conduct operations.[7] This role was eventually codified on 25 April 1985, when the Chiefs of Staff of the US Army and US Air Force collectively agreed that the Army held the responsibility to defend air bases so that the Air Force could generate and sustain air power.[8] The resulting document was Joint Service Agreement (JSA)-8.

Throughout most of its history, the US Air Force rested upon the belief that protection of an airfield's exterior perimeter was a soldier's responsibility, while Airmen had passive defense inside the perimeter.[9] JSA-8 cemented this belief for many years with its intent being to guide the development of regulations, publications, and joint doctrine for ground defense of Air Force bases.[10] It recognized the Army's "fundamental role in land combat and the requirement to protect the Air Force's ability to generate and sustain air power for joint air-land combat operations."[11]

To this end, JSA-8's operating guidance attempted to codify Air Force roles and responsibilities for Air Base Ground Defense (ABGD) forces by directing specific defense-response capabilities. For example, ABGD personnel had to be capable of detecting and defeating what was then considered Levels I, II, and III attacks. In general, level I included terrorist and sabotage attacks, while Level II included diversionary and sabotage operations by "unconventional forces, raids, ambushes, and reconnaissance by force missions."[12] Level III attacks encompass enemy action by battalion-sized forces or greater and required ABGD forces to hold off the attack until Army tactical units could arrive in support.[13] The terms of JSA-8 assigned the Army with ABGD outside the air base, whereas the Air Force held internal defense duties.[14]

---

[7] Palmer, "Air Base Security Operations," 1.
[8] Chief of Staff US Army and Chief of Staff US Air Force, Joint Service Agreement, 25 April 1985, K168.7267-119, 21 Dec 84 – 13 Dec 85, in USAF Collection, AFHRA.
[9] Palmer, "Air Base Security Operations," 46.
[10] Palmer, "Air Base Security Operations," 23.
[11] CSA and CSAF, "JSA-8"
[12] Palmer, "Air Base Security Operations, 23-24
[13] Palmer, "Air Base Security Operations" 23-24.
[14] Palmer, "Air Base Security Operations," 24.

Air Base Ground Defense was not an attempt, however, at building an Air Force infantry battalion. "In the past…SF leaders thought this BCT [Army Brigade Combat Team] or this MEU [Marine Expeditionary Unit] would handle a base's external threat because they were adjacent to the base. The fluid nonlinear battlespace erases the old lines. Now the base is an "autonomous joint operating area" and may not have joint ground forces linked to it."[15]

Ultimately, JSA-8 failed to gain traction amongst the services and "was never fully implemented or developed."[16] Both services agreed to abrogate the agreement on 24 March 2005 and designated the decisions of the Joint Force Commander as the reigning authority for air base defense in JSA-8's absence.[17] The cause of the abrogation was largely an issue of Army force readiness and health during the Global War on Terrorism (GWOT), although there is some debate that the document was a paper tiger from its onset, and the Army never fully intended to accept the mission.[18] Setting this debate aside, it is known that the GWOT nearly broke the Army; significant decline in recruitment and retention, coupled with extended combat deployments placed considerable stress upon available forces, necessitating changes to operational constructs.[19]

As a result, the Army turned to the Air Force for help with its ground commitments. This afforded a reallocation of ground combat elements. After all, "An army consumed with self-protection cannot harm the enemy."[20] With the Air Force taking responsibility for air base defense, the Army could free up valuable resources for other priorities that support gaining and maintaining land power.

---

[15] Rebecca Grant, "The Security Forces Rewrite," *Air Force Magazine* 89, no. 1 (Jan 2006): 57. http://www.airforcemag.com/MagazineArchive/Pages/2006/January%202006/0106security.aspx. Accessed 18 March 2014.

[16] Palmer, "Air Base Security Operations," 24. Here, Palmer is quoting Brig Gen Robert H. Holmes, [then] Director of Security Forces and Force Protection and the staff summary sheet to AF/CC, "*Package (BLUE) XOS-F.041118.1 Validating the Abrogation of Joint Service Agreement 8",* 18 Nov 04

[17] Palmer, "Air Base Security Operations," 24.

[18] Michael Kifer, Deputy Director, PACAF A/7S, emails with author

[19] Palmer, "Air Base Security Operations," 1.

[20] Brig Gen (ret) Huba Wass de Czege, Maj Jacob Biever, "Force Protections: from Fort to Foxhole, *Army Magazine* 51, no. 6 (June 2001). http://www.ausa.org/publications/armymagazine/archive/2001/6/Documents/FC_de_Czege_0601.pdf, accessed 18 March 2014.

How Ground Doctrine Affects the Air Base

Landpower, according to U.S. Army Field Manual (FM) 3-0, is "the ability – by threat, force, or occupation – to gain, sustain, and exploit control over land, resources, and people. Landpower includes the ability to support and provide a base from which joint forces can influence and dominate the air and maritime domains of an operational environment." [21] Although the aim of landpower remains unchanged, the environment in which it is exercised has undergone significant changes in the post-9/11 landscape. Today's operations are "increasingly distributed in space while more simultaneous in time."[22]

Furthermore, at the tactical and operational level, subordinate units "routinely operate in noncontiguous areas of operations. This contrasts sharply with the "contiguous and hierarchical arrangement of land forces in the past."[23] The benefit of contiguous operations was the shared boundary easily separating and distinguishing areas of operations; noncontiguous areas do not have such a boundary.[24] Contiguous areas of operation represent the traditional approach to air base defense and are a remnant of the conventional Cold War threat.[25] They represent the linear battlefield of the past, which may only find resurrection in a confrontation against a near-peer adversary.[26]

Consequently, Army planning in the Cold War era and after focused on deep, close, and rear areas of operations and security. A battlefield often consisted of forces conducting linear operations that were coordinated with nearby units. These shared boundaries clearly established front and rear echelons which clarified the roles and responsibilities of support forces and afforded zones of security for rear areas. Additional information provided in figure 3.

---

[21] Headquarters, Department of the Army, FM 3-0, "Operations," Feb 2008, p. 1-17
[22] Army, FM 3-0, "Operations." C-1.
[23] Army, FM 3-0, "Operations." C-3.
[24] Army, FM 3-0, "Operations," 6-1.1.
[25] Gray, Ron. "Integrated Swarming Operations for Air Base Defense: Applications in Irregular Warfare," Naval Postgraduate School, June 2006, 1.
[26] Sagraves, "Air Base Defense," 10.

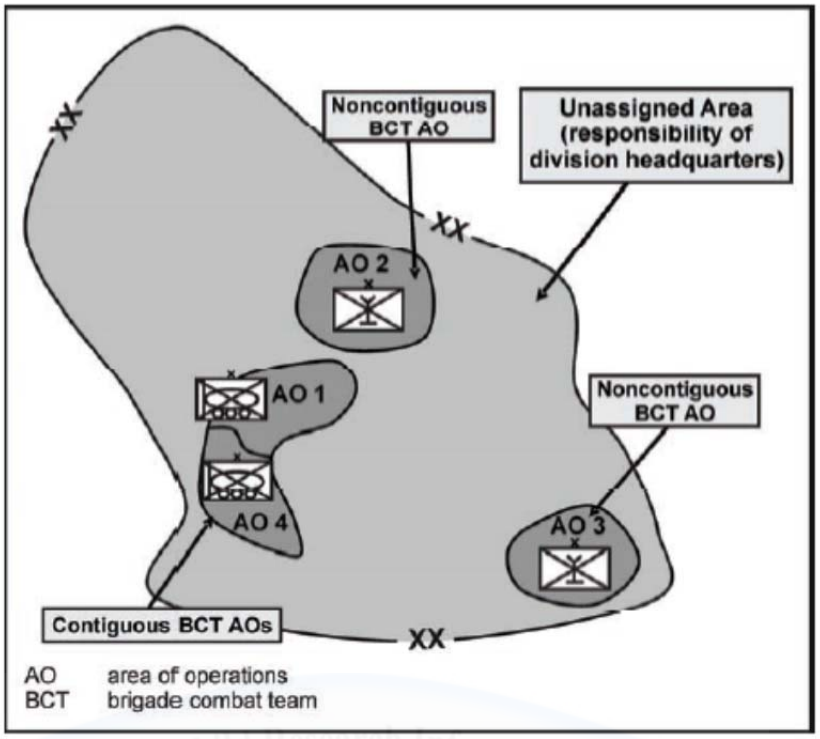

Figure 3. FM 3-0, Contiguous, Noncontiguous, and Unassigned Areas
Source: Hq US Army FM 3-0, "Operations", 6-11

Current Army doctrine, however, rescinds deep, close, and rear areas, as well as linear and nonlinear array of forces on the ground.[27] Its doctrine now organizes the battlefield according to function, focusing on decisive, shaping, and support operations as part of a larger, modular force. These changes stem from more agile forces, improvements to command and control capabilities, and increased integration of joint capabilities at lower echelons.[28] The 2001 version of FM 3-0 reflected the Army's belief that nonlinear operations are "now more common than ever."[29]

Further, these revisions addressed a changing enemy and changing nature of war, specifically, irregular war and battles focusing less on terrain and more on undermining the actions of the enemy. Said otherwise, it was adaptation to a different threat. During the Cold War, the enemy operated with greater predictability, with more readily

[27] Army, FM 3-0, "Operations," D-4.
[28] Army, FM 3-0, "Operations," C-1.
[29] Sagraves, "Air Base Defense," 12

identifiable logistics and support mechanisms, and typically remained at or beyond the Forward Edge of the Battle Area (FEBA).

Today's conflicts give rise to "super empowered individuals" versus more traditional state-on-state conflict.[30] When the enemy encamped near the FEBA, it took little time to locate him, but greater effort to kill him. Today's irregular conflicts invert this trend, requiring considerable effort in locating the enemy, but less difficulty engaging him.[31] Though Army doctrine replaces nonlinear with noncontiguous, the message remains consistent; clean, neat lines of contiguous operations are less likely in contemporary conflicts.

This change carries significant ramifications for airmen and air base defense plans as Army doctrine no longer guarantees its role of providing base defense and perimeter security. "The contiguous arrangement of the AO (area of operations) means that there are no exploitable gaps between adjacent ground units, reducing the likelihood of an undetected penetration by infiltrating enemy forces. The chance of ground attack against an air base in this situation is exceedingly remote."[32] Furthermore, a transition to noncontiguous operations creates seams in the battlefield arrangement. These result from the disparate maneuvers of friendly ground forces which no longer arrange under contiguous lines. As a result, large areas of operation remain disconnected and potentially undefended; these less-policed areas provide the enemy with increased areas to stage operations against an air base.

The shift away from contiguous operations is not a punitive action against the Air Force, but an extension of changes in the Army's battlefield doctrine and the nature of current conflicts. As Brigadier General Holmes appropriately summarized, "There is no rear area…in particularly [sic] now as we see in Iraq, so it's not a matter of air bases will be in the rear area so therefore they're safe and sound…Air bases are on the front line. Our airmen, just in doing things in and around, outside the perimeter of the base, find that they're in a high-threat, high-risk area. So…the ballgame has changed."[33]

---

[30] Michael Kifer, Deputy Director, PACAF A/7S, emails with author
[31] Kifer, emails with author
[32] Sagraves, "Air Base Defense," 17
[33] Sagraves, "Air Base Defense," 10

Clarifying Standoff Doctrine

Protecting and defending an air base requires its own strategy, employing numerous Air Force capabilities in a variety of ways, the successful implementation of which ensures commanders deliver desired effects. In the case of an integrated air base defense, the Installation Commander is responsible to "identify risks and develop risk management strategies to produce effects-based, integrated defense plans" that ensure unhindered support to the mission.[34] This requires an integration of offensive and defensive capabilities that mitigate threats against the air base. More specifically, integrated defense concerns operations within the base boundary and base security zone.[35] These terms carry specific implications for integrated defense of an air base; an explanation for each is illustrated below for further understanding.

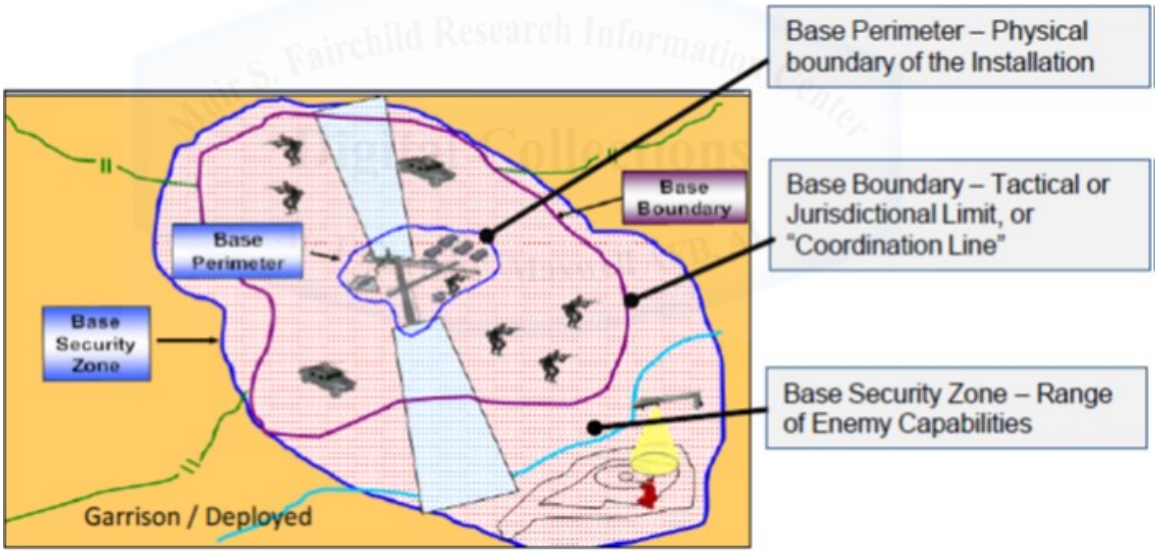

Figure 4. Integrated Defense Concept
Source: Hq US Air Force, AFPD31-1, 28 October 2011, p. 3

The base perimeter represents the physical boundary of the installation.[36] It encapsulates the hub of activity for the installation, enveloping its operational units and support facilities. Most importantly, the base boundary (BB) is not necessarily the base

[34] Hq USAF, Air Force Policy Directive 31-1, *Integrated Defense*, 28 October 2011, 2.
[35] AFPD 31-1, *Integrated Defense*, 2.
[36] AFPD 31-1, *Integrated Defense*, 11.

perimeter. These are important distinctions to make, as the amount of land area can vary considerably between the two terms and BB was constructed to take into consideration the standoff threat. Depending on the standoff threat, the base boundary may remain close to the base perimeter, but in general, there is a directly proportional relationship between the base perimeter and the base boundary with regard to the standoff threat. In other words, the greater the standoff threat, the greater the surface area of the base boundary. (see lower right quadrant of figure 3) To counter the risk of getting lost in verbiage, in the words of one expert, "the Base Boundary is the ONLY thing that matters."[37]

[37] Kifer, emails with author, 5 March 2014. [emphasis in original]

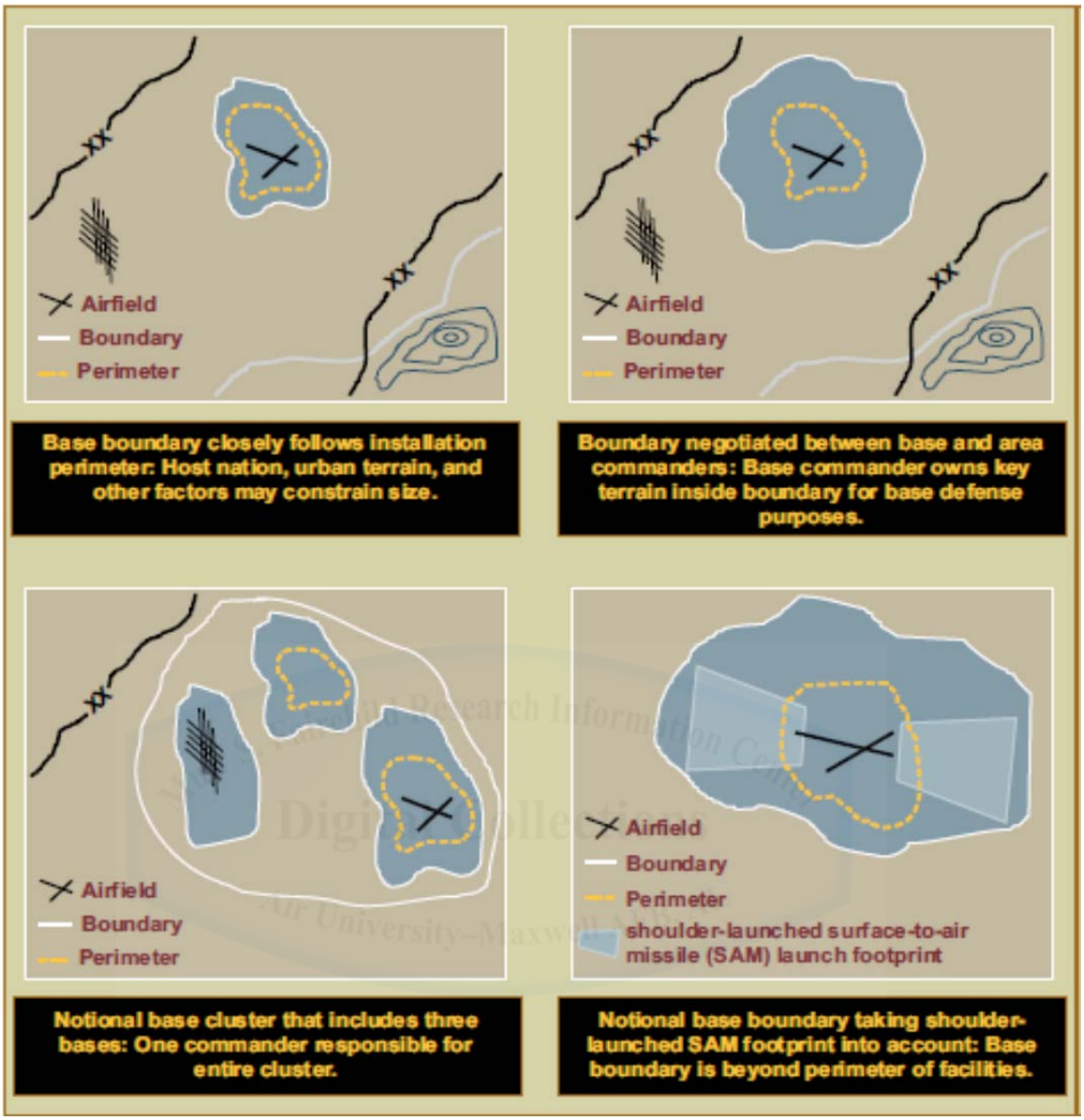

Figure 5. Base Boundary Considerations
Source: US Joint Chiefs of Staff, Joint Security Operations in Theater, *Joint Publication 3-10 (Washington, DC: US Joint Chiefs of Staff, February 3, 2010), IV-4.*

The base security zone (BSZ), on the other hand, is an Air Force-specific term to be used intra-service only and describes the area of concern around an air base to support the establishment and adjustment of the base boundary.[38] The BSZ also refers to the range of enemy capabilities, in that it represents the area outside the base by which mortars, rockets, MANPADS, etc. can reach the base and increase its vulnerability.[39] Said

[38] AFPD 31-1, p.11.
[39] AFPD 31-1, p.11-12.

otherwise, the BSZ is a planning construct for the area outside the base boundary. Based upon the intelligence estimate, it represents the ground a commander wants to dominate through use of his own forces, or through negotiation with the battle space owner, Joint Force Land Component Commander, host nation military, host nation police, etc.[40]

The distinction between BB and BSZ is important to base defense because it requires close coordination between affected units and commanders, implying that poor coordination or command and control may increase risk. Additionally, these terms identify and segment what is potentially a great deal of terrain requiring considerable assets to secure and protect – assets that are often in short supply but high demand. Therefore, the foundation of a strong base-defense plan is the proper allocation of resources. Absent the right resources, base assets assume a greater risk. Jeffrey Vish offers a pertinent analogy: hit an aircraft with a sledgehammer, you can do hundreds of thousands of dollars in damage with each blow and, in a short time, make it unflyable and possibly put it beyond repair. Hit an M-1 tank with a sledgehammer and you hurt your hands.[41] Properly understanding and coordinating assets in support of BB and BSZ can metaphorically yield tank-like strength to an air-base-defense posture.

Understanding the Standoff Footprint

As the USAF transitions away from A-10s and F-16s toward F/A-22s and F-35s, we continue the journey of reliance upon very expensive aircraft. Although each of the latter airframes provides incredible lethality, it comes at a corresponding unit-per-copy cost, as well as in-theater maintenance cost. Specifically, the stealth aspects of F/A-22s and F-35s mean that damage to the exterior becomes increasingly complicated and costly to repair. If the damage happens in Afghanistan or other locations lacking a robust air-defense network, the stealth capability of the aircraft may not be needed, and a risk assessment may allow for continued flight. However, if the damage is structural, the high-tech nature of the airframe will translate to increased downtime as a product of longer repairs. With a reduction in overall quantity of aircraft, each copy must assume a greater role in air operations. Should a standoff attack render an aircraft unfit for flight,

[40] Kifer, emails with author, 5 March 2014.
[41] Jeffrey Vish, "Guided Standoff Weapons: A Threat to Expeditionary Air Power," Naval Postgraduate School, September 2006, 12.

there is a significant interruption in sortie production and the subsequent ability to project air power. As such, countering the standoff threat grows in importance as our reliance upon high-tech airframes increases.

Countering standoff threats is increasingly difficult against enterprising enemies making use of available technology. As range favors the attacker through weapons with greater reach, the security perimeter around an airbase grows substantially. (refer to previous correlation between BB, BSZ, and standoff threat) Generally, an increasing security perimeter requires a corresponding increase in resources. Additionally, distances and complexity of attack are directly proportional. Increasing the distance between the defensive resource and where an adversary can stage an attack increases the complexity of the methods the attacker must use.[42]

For example, it is easier to hit a target at twenty meters with a hand grenade than a target at 2,000 meters using a sniper rifle. The tradeoff comes in ease of access; getting within twenty meters of a target is considerably more difficult, especially if the target is inside a fortified base perimeter. This leads to a desire for greater standoff reach. With this reach comes ease of attack for the adversary, but difficulty in defense for the base.

As an example, presume an adversary makes use of an 82mm mortar round with a range of eight kilometers. Using the formula for the area of a circle ($A = \pi r^2$), this equates to an area of defense of 201 square kilometers from each potential target.[43] Converting kilometers to miles, this is roughly 77 square miles, or an area equal to Cleveland, OH.[44] Using a 120mm mortar round with an approximate range of seven kilometers means a standoff footprint of roughly 58 square miles.[45] This is an area roughly the size of Fayetteville, NC.[46] In short, a weapon with just a few miles of standoff reach for an attacker will translate to a base boundary area for the defender to secure equal to or greater than many populous US cities.

Defending an area this large requires a significant expenditure of manpower – a resource that is normally provided by the Army. It should be expected that only a small

[42] Vish, "Guided Standoff Weapons," 12
[43] Vish, "Guided Standoff Weapons," 11
[44] US Census, "County and City Data Book," 726. Cleveland is approximately 77 sq miles in area. http://www.census.gov/prod/2008pubs/07ccdb/ccdb-07.pdf, accessed 26 March 2014.
[45] Sagraves, "Air Base Defense," 35
[46] US Census, "County and City Data Book," 725

portion of the Army's total combat power will be allocated or dedicated to duties such as perimeter and area security in support of air base defense.[47] As a result, the size of the corresponding base boundary will depend upon the known capabilities of an adversary at that time, based upon METT-T considerations.[48] If resources are scarce or are otherwise dedicated, a decision must be made to accept additional risk or allocate resources in an effort to minimize it. This is a difficult decision that will require close monitoring of the intelligence environment to assess the threat, and closer coordination with affected support agencies and units likely to be tasked with area security.

Conclusion

Previous doctrine entrusted the Army with air base security and defense. Expeditionary operations, especially in an irregular war, do not fit the Cold War model this doctrine addresses, as partly evidenced by the abrogation of JSA-8. Instead, expeditionary and irregular warfare creates a noncontiguous battlefield where the US Army no longer establishes front and rear areas. Currently, the Army focuses on main and supporting efforts for ground operations, eliminating the front and rear area of security and the delineation they provided. Absent this delineation, high-value aircraft and equipment will operate in areas not protected by traditional security boundaries yet will still require robust defense postures. In expeditionary locations, the USAF may discover the role of air base defense being placed upon its airmen and aircraft when the task previously fell upon the Army.

Due to a historical precedent of air base attacks, as well as a known deficiency in perimeter security as it relates to mitigating standoff attacks, it is critical that the Air Force establish the proper security posture to defend the air base. Its power-projection assets remain paramount in combat operations, and the need for an adequate defense is similarly important against a clever and resourceful adversary using irregular warfare tactics. This risk is elevated when Army operations do not establish a secure area for air

[47] Sagraves, "Air Base Defense," 35.

[48] JP3-10, II-2. "The base boundary…should be established based upon the factors of mission, enemy, terrain and weather, troops and support available – time available (METT-T), specifically balancing the need of the base defense forces to control key terrain with their ability to accomplish the mission."

operations, or does not apportion assets for air base defense. Given these considerations, leadership should continue exercising diligence with regard to force protection and air base defense when conducting expeditionary operations.

Furthermore, as the Air Force draws down close-air-support platforms such as the A-10 and F-16 and transitions to stealthy platforms like the F/A-22 and F-35, there will be an increasing difficulty in repairing damage caused by standoff attacks. A delay in repair immediately correlates to an interruption in sortie production and thus, power projection. History reveals that a capable and willing adversary is more likely to disrupt air operations than attempt to defeat or overrun an air base. So long as this holds true, standoff weapons and tactics will remain the attack method of choice.

Countering the standoff footprint requires considerable resources; resources that may not be readily available for the task of air base defense. A shrewd enemy knows this and will attempt to encroach upon the standoff footprint and attack the air base by myriad techniques. The question then becomes: will the previous use of rockets, mortars, and sniper attacks continue, or will the enemy transition to guided platforms such as small-scale RPAs? The next chapter addresses this challenge.

Chapter 4

SMALL-SCALE RPAs: HISTORY, USE, AND OUTCOME IN WAR

Introduction

Even before heavier-than-air powered flight became a reality for the Wright brothers in 1903, early theorists envisioned the military advantages to be gained by taking to the skies and using aerial craft as weapons of war.[1] From the skies, a commander's force of aircraft could gain a position of advantage and leap over and beyond terrestrial armies, bypassing the barriers posed by land and water.[2] As the use of airplanes grew and their technology developed, theories guiding their military use advanced as well. The promises of air power seemed endless; in theory, airpower could take use of the space above the earth to decide the outcome of war being fought on the surface.[3] Taking to the air signaled a new means by which you could exact pain and violence upon your enemy.

In 1915, German Zeppelins began a series of attacks on London and the English countryside. The falling bombs terrorized the population, causing two thousand civilian casualties and hundreds of millions of pounds' worth of damage.[4] The physical and psychological damage of the attacks was exactly what the Germans desired; but, beyond the fear and panic, the attacks meant much more. England, seemingly insulated by her surrounding waters, suffered an attack for the first time since William the Conqueror's invasion in 1066.[5] The proud British Navy was helpless to stop the attacks, and it became apparent that taking to the skies could finally bypass the "stopping power of water."[6]

Over time, history would make abundantly clear that the use of the aircraft did not remain isolated to military operations, and civilian applications grew considerably over the coming decades. While other means of transportation such as railways and ships

---

[1] Joseph Harahan, Richard Kohn; Editor's Introduction of "The Command of the Air" by Giulio Douhet, University of Alabama Press (Tuscaloosa, AL: 2009), 1.
[2] Harahan and Kohn, "The Command of the Air," 2.
[3] Harahan and Kohn, "The Command of the Air," 2.
[4] Sam Howe Verhovek, *Jet Age: The Comet, the 707, and the Race to Shrink the World* (New York: Avery, 2010), xvii, 62-63.
[5] Verhovek, 62.
[6] John J. Mearsheimer, *The Tragedy of Great Power Politics*, The Norton Series in World Politics (New York: Norton, 2001), 84.

remained important, the aircraft grew in popularity. In fact, for many years, more Americans crossed the Atlantic Ocean by ships than airplanes, though this would change by the late 1950s and early 1960s, allowing the reversal of fortune to favor airplanes.[7] While the aircraft gained popularity with each passing year, an interesting but subtle development took place: the continued development of unmanned aircraft.

At first glance, it may appear odd that unmanned aircraft held any part of the aviation discussion, especially while manned platforms grew so quickly in prominence. Further, the use of unmanned aircraft in contemporary operations may lead many to believe the concept is a recent development and that RPAs are only a few years old. In truth, unmanned platforms have a storied and diverse history dating back as far as the US Civil War and earning a unique place alongside Hollywood legends.[8] World War II, Korea and Vietnam saw various applications of RPAs as well. So long as there have been manned airplanes fighting in combat, unmanned variations were also present, albeit in more infantile stages of development and use. The distinction here is important: for all the potential and advantages of the manned aircraft, unmanned variants stood to deliver similar benefits without a corresponding risk to the pilot. The limitations of technology, however, would ultimately make unmanned platforms less appealing when compared to more capable manned platforms. While manned aircraft took center stage, unmanned technology sat silently in the shadows, awaiting the opportunity to prove its worth.

In assessing RPA utility, it is vital to understand that unmanned aircraft are aircraft all the same. While they may lack many of the traits of specific manned platforms, such as the cargo capacity of a C-130, unmanned aircraft are not without merit, especially in a wartime setting. Unfortunately, the development of RPAs over time remained consistent in theoretical application but fell short in realistic performance. In this regard, it reflected the same growing pains of air power, writ large. Air power critics often complained of

---

[7] Verhovek, xvii. Verhovek claims that in the US, the ten largest transportation companies in 1958 were all railroads and that fewer than one in ten American adults had ever been on an airplane. In 1958 and beyond, the balance shifted toward aircraft.

[8] Jim Garamore, "From U.S. Civil War to Afghanistan: A Short History of Uavs," Defense.gov, April 16, 2002, accessed April 8, 2014, http://www.defense.gov/news/newsarticle.aspx?id=44164. For more on the Hollywood aspects of early RPAs, see P W. Singer, *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century* (New York: Penguin Press, 2009), 49-50., and the creation of the Dennymite aircraft and role early RPAs played on the introduction of Marilyn Monroe.

over-promising and under-delivering, though time ultimately reveals evidence for a worthy rebuttal to the argument. With RPAs, many of the same vexing themes of air power development persisted: theory rarely became reality (more on this in subsequent sections). In many instances, the available technology at the time was the limiting factor. That does not necessarily invalidate the theory, however. Rather, the ways of thinking about and using RPAs remained rather consistent over time and ultimately bore fruit in Vietnam and even more so in Iraq and Afghanistan. This makes one ponder their utility given even more time for them to develop and mature.

Once capable, RPAs found use in many of the same applications posited by original air power theorists. Historically, RPAs were scaled-down or actual versions of production-scale aircraft, modified for use without an onboard aircrew or pilot. Now, technology is advancing at such a pace as to afford much smaller platforms with the same, or even superior, payload, range, and loiter time of full-sized aircraft. As this trend continues, smaller RPAs successfully incorporate ISR capabilities that provide for intelligence-gathering without the consequential need for a dedicated runway. In his book, *Astropolitik: Classical Geopolitics in the Space Age*, Everett Dolman states, "Despite the fact that aircraft were essentially unimpeded by the Earth's surface features…they were limited in their operations by critical *air operations routes*, which required precisely located takeoff and landing fields and effective maintenance and repair facilities at major hubs."[9] Dolman uses this claim to support his argument in the overall context of space-based operations, his point remains valid for today's air power operations. Ultimately, air operations require adequate locations, criteria for which make their locations limited and predictable. Small-scale RPAs potentially avoid these requirements and continually advancing technology implies they can deliver tactical effects similar to full-size aircraft without the consequent infrastructure. In short, this blends mobility and capability in ways that could prove detrimental to US interests abroad.

[9] Everett C. Dolman, *Astropolitik: Classical Geopolitics in the Space Age*, Cass Series--strategy and History (London: Frank Cass, 2002), 43. Emphasis in original.

A Brief History of RPAs

While this section does not attempt to catalog all RPAs over the last one hundred years, it does attempt to capture the philosophy of their growth and development while extrapolating their relevance for contemporary and future operations. As mentioned above, many of the early attempts of unmanned aircraft fell short of desired performance. This section seeks to capture some of the growing pains experienced over time and demonstrate how RPA capability is advancing rapidly and is shedding many of its previous limitations.

American unmanned platforms date as early as the Civil War, with Confederate and Union forces attempting rudimentary use of explosive-laden balloons intended to come down within a supply or ammunition depot and detonate. ("It wasn't terribly effective.")[10] While balloon-assisted devices began in the 1860s, powered mechanisms developed during World War I with the Kettering Bug.[11] Invented in 1917, the Kettering Aerial Torpedo, later nicknamed the "Bug," was relatively small with a wingspan just shy of 15 feet with a range of 75 miles and gross weight of 530 pounds loaded. The Bug was one of the earliest manifestations of the desire to achieve air power effects without the corresponding risk to a pilot. Far from the level of control and precision guidance characteristic of today's RPAs, the Bug had pre-set pneumatic and electric controls for stabilization and launched from a portable track. Once it arrived near the target, it would kill its engine, shed its wings and plummet toward the ground, carrying 180 pounds of explosives that would detonate on impact with the target. Fewer than 50 Bugs were built before the Armistice, and none saw combat.[12]

In the interwar years and into World War II, several RPA versions existed, including B-17 and B-24 aircraft used during the once top secret Operation Aphrodite. The Aphrodite program made great strides beyond earlier WWII iterations (the Japanese experimented with explosive-laden balloons briefly before giving up) and used modified

---

[10] Jim Garamore, "From U.S. Civil War to Afghanistan: A Short History of UAVs", 16 April 2002, American Forces Press Service, http://www.defense.gov/news/newsarticle .aspx?id=44164, accessed 8 April 2014. Here, Garamore quotes Dyke Weatherington, deputy of the Defense UAV Office.

[11] National Museum of the US Air Force (NMUSAF), *Kettering Aerial Torpedo "Bug"*, http://www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=320, accessed 7 April 2014.

[12] NMUSAF, *Kettering Bug*

manned aircraft as a type of cruise missile.[13] For these missions, a full-scale aircraft would take off and navigate by manned aircrew, gain the appropriate elevation and bearing and then get handed off to a separate aircraft for final navigation to the target. Once acquired by the adopting aircraft, the originating aircrew would bail out, effectively turning the previously manned aircraft into a guided projectile. Historians and conspiracy theorists may recall Operation Aphrodite for the fame it garnered when US Navy Lieutenant Joseph P. Kennedy (President Kennedy's older brother) died when his bomber suddenly exploded after takeoff in 1944.[14] Unsuccessful results led to Aphrodite's cancellation in 1945.

In 1939, the nation was still recovering from the Great Depression and the US Army ranked 39th in the world, vastly behind contemporaries in overall strength and relying on horses to pull artillery pieces.[15] In the wake of Pearl Harbor, President Roosevelt set staggering industrial production goals in order to out-produce and out-equip the Germans and Japanese: 60,000 aircraft in 1942 and 125,000 in 1943.[16] As a result, many American industries underwent substantial industrial conversion to support the war. Chrysler converted operations to make fuselages; General Motors made airplane engines, guns, tanks, and trucks; and Ford assembled all 1,550,000 parts of the B-24 Liberator to roll a whole aircraft off the line every 63 minutes.[17] The Louisville Slugger baseball bat company began producing M-1 carbine stocks, tank pins, and billy clubs for the armed forces.[18]

While these may be interesting bits of trivia, the larger issue was that private sector of industry threatened to collapse without government support. Though the civil sector benefitted from government intervention, it posed a novel problem of policy "suggesting that separation between the public and private sectors was obsolete."[19] Glancing into the future, this posits the reliance between government-sponsored research and development

[13] Garamore, "Short History of UAVs"
[14] Garamore, "Short History of UAVs"
[15] Author Unknown, "At Home War Production," PBS.org, April 10, 2014, accessed April 10, 2014,http://www.pbs.org/thewar/at_home_war_production.htm.
[16] Author Unknown, "At Home War Production.
[17] Author Unknown, "At Home War Production.
[18] Louisville Slugger Museum and Factory, "Our History," http://www.sluggermuseum.com/about, accessed 8 April 2014.
[19] McDougall, 88.

and RPA survival and growth; in order to thrive, will state-sponsored intervention be a prerequisite? It is conceivable that commercial-market growth alone may sufficiently supplant government intervention to allow small-scale RPAs to progress in the technology upon which they rely. Commercial products may provide the impetus to propel this technology and provide users with a menu of off-the-shelf options.

After WWII, the American armed forces continued to hone and improve unmanned platforms. In Korea, the Far East Air Forces suffered disappointing results using guided munitions, though they failed to discourage the Navy from further experiments. In August and September, 1952, the Navy launched six F6F-5K Hellcat drones off the USS Boxer for targets in North Korea.[20] These aircraft navigated by way of television camera instead of a pilot and carried a significant payload, intending to deliver a one-ton bomb upon their targets.[21] Similar to the Aphrodite concept, once the Hellcats launched they received guidance from an adopting ship that guided the Hellcat via radio control.[22]

In a bit of reporting that now appears prescient, a news report entitled, "Navy Launches Robot War," proclaimed the dawn of a new era of warfare, describing "guided missiles for the first time in combat, bringing the push button war of tomorrow into present day reality."[23] The narrator of the segment speculated that these new robot bombers might "someday eliminate the human element from air war."[24] Much like the Aphrodite missions, the Hellcat attempts proved just as unsuccessful. In this regard, there is a parallel path between the growth of unmanned platforms in a wartime setting and the zeal of a public seeking a different humanity in war. The debate continues today with each side seeking answers to the questions that vex it.

Following Korea, Cold War tensions escalated. In 1960, the USSR shot down Francis Gary Powers during a U-2 mission, prompting President Eisenhower to suspend U-2 operations. This left the United States without a vehicle to monitor and observe Soviet activities. Following this decision, the Technological Capabilities Panel met to

[20] Conrad C. Crane, *American Airpower Strategy in Korea, 1950-1953*, Modern War Studies (Lawrence, KS: University Press of Kansas, 2000), 134.
[21] Crane, 134.
[22] Crane, 134.
[23] Crane, 134.
[24] Crane, 134.

examine feasible options to replace the high-altitude U-2.[25] The panel expressed an interest in unmanned platforms for espionage missions and turned to the Ryan Aeronautical Company, a maker of Firebee target drones.

In the first attempt, Firebee drones were converted into reconnaissance platforms, but had disappointing results, and a redesigned version of the Ryan Model 147A "Lightning Bug" was then put into use.[26] The Lightning Bug had a longer wingspan than the Firebee and could reach an altitude of 50,000 feet while its onboard camera was capable of securing one to two feet of imagery resolution.[27]

The CIA continued experiments with different unmanned platforms, eventually developing a remotely controlled dragonfly that could land on buildings and record conversations taking place inside, given it could navigate through anything more than a subtle breeze.[28] It is worth using this timeframe as a bookend for the development of unmanned platforms; micro-scaling of materials and technology offered great diversity in the applications of unmanned platforms. Time and technology both progressed in a manner that allowed a better bond between theoretical use and technical realism. In short, technology came of age, and unmanned platforms became more successful.

Cold War technology enabled a significant use of unmanned platforms as the conflict escalated for US forces in Vietnam. While students and veterans of Vietnam still grapple with the historical and political implications of the conflict, few likely relate this tumultuous period with technological advances in RPAs. The Cold War Firebee drones, which previously fell short of expectations, saw extensive use in Vietnam and successfully flew over 3,400 surveillance missions.[29] Cementing their diversity and utility, Firebees were used for night-photo missions, COMINT and ELINT applications, leaflet dropping and surface-to-air missile radar detection, location, and identification throughout the conflict.[30]

Previously, RPAs served as a type of technology demonstrator or proofs of concept.

---

[25] Dino A. Brugioni, *Eyes in the Sky: Eisenhower, the Cia, and Cold War Aerial Espionage*, ed. Doris G. Taylor (Annapolis, Md.: Naval Institute Press, 2010), 223.
[26] Brugioni, 223.
[27] Brugioni, 223.
[28] Brugioni, 319. Interestingly, the CIA also saw fit to create remotely controlled catfish.
[29] Garamore, "A Short History of UAVs"
[30] Garamore, "A Short History of UAVs"

The more immediate benefit was the absence of a pilot at risk, but Vietnam usage helped cement second and third-order effects. First, RPAs cost significantly less than full-size aircraft, meaning they were easier to reproduce and were expendable. Second, as they were much smaller than airplanes, UAVs (Firebees, in particular) were much harder to detect and target. A Boeing 707 platform, for example, was far easier to detect than an RPA a fraction of its size.[31] RPAs finally became cost-effective substitutes for certain niche missions typically executed by manned platforms.

At this point in history, full-size RPAs primarily focused on ISR capabilities versus being armed for kinetic effects like the Predator or Reaper platforms we know today. There is, however, considerable transfer value from the traits learned in Vietnam to the traits witnessed with today's small-scale units. Namely, small-scale RPAs are still difficult to track and target, which not only makes them an appealing asset for friendly forces, but consequently provides the same advantage to the enemy. If an adversary gains a position within standoff distance and launches a difficult-to-detect aircraft, this concealment potentially grants sanctuary and mitigates risk in the attack. One of Murphy's Laws of Combat sardonically poses that tracer bullets work both ways. Similarly, our defensive posture must account for an RPA that is difficult to detect and target, as it offers the same advantage to both sides of the fight.

After Vietnam, American RPA development took a clue from Israeli programs which had aggressively pursued unmanned technology. The US Navy and Marine Corps Pioneer system went into operation in 1985 and is a derivative of Israeli developments.[32] During Operation Desert Storm, the Pioneer acted as a forward scout and helped guide the 16-inch guns of the *USS Missouri* battleship onto targets on Faylaka Island off the coast of Kuwait City.[33] In an interesting tale of the war, shortly after the devastating assault on Faylaka Island, US Navy operators on the *USS Wisconsin* intentionally flew the Pioneer over surviving enemy troops. Upon hearing the two-cycle engine, Iraqi forces began surrendering, presuming the Pioneer's presence meant an imminent barrage of navy shelling, even though the *Wisconsin* was over the horizon and invisible to Iraqi

[31] Keith L. Shimko, *The Iraq Wars and America's Military Revolution* (New York, NY: Cambridge University Press, 2010), 42.
[32] Garamore, "A Short History of UAVs"
[33] Garamore, "A Short History of UAVs"

forces.[34]

The Gulf War signaled the coming of age of unmanned systems, and American military leadership soon began to recognize their potential value on the battlefield. Shortly thereafter, the MQ-1 Predator system emerged from an Advanced Concept Technology Demonstration project to find use in the Balkans conflict.[35] The Predator, flying between 15,000 and 25,000 feet, underwent significant modifications from the post-Gulf War era until today, moving from a strict ISR platform to a dual-role missile-delivery and ISR asset. The MQ-9 Reaper and RQ-4 Global Hawk are close relatives of the Predator and illustrate a progression in performance capability, but the larger issue is how these collective technologies began shaping the character of war, versus merely trying to find a viable role in war.

According to Clausewitz, war is an act of force to compel our enemy to do our will.[36] In this sense, the *nature* of war is unchanging. Mark Bowden makes a careful distinction about the *character* of war being changed by UAVs, specifically the Predator.[37] The nature and character of war are nuanced, where the character is altered by iterations in technology such as gunpowder, improved rifles, advancements in propulsion for ships and aircraft plus many others. These advancements, while noteworthy, do little to change the nature of war and the duel inherent in Clausewitz's war. "The invention of gunpowder and the constant improvement of firearms are enough in themselves to show that the advance of civilization has done nothing practical to alter or deflect the impulse to destroy the enemy, *which is central to the very idea of war*."[38]

The Predator, in particular, showcased the progression of technology in a way that altered the character of war by its integration to other wartime tools. Originally, the Predator linked its video feed only to the operators on the ground. After the sustained fight in Iraq and Afghanistan, the Predator linked its camera feed into the global telecommunications system where it could be piloted – and its live feed viewed and

[34] Garamore, "A Short History of UAVs"
[35] Garamore, "A Short History of UAVs"
[36] Carl von Clausewitz, *On War*, trans. Michael Howard, Peter Paret, and Bernard Brodie (Princeton, N.J.: Princeton University Press, 1984), 75.
[37] Mark Bowden, "How the Predator Drone Changed the Character of War," *Smithsonian Magazine*, November 2013, 1, accessed April 9, 2014, http://www.smithsonianmag.com/history/how-the-predator-drone-changed-the-character-of-war-3794671/?all.
[38] Clausewitz, 76. Emphasis added.

missiles fired – from any location in the world.[39] The overwhelming capability placed additional demand on the system, and senior military leaders wanted continual airborne coverage, or "caps." Doing so continually allowed US forces to monitor enemy movements and communications day or night, significantly enhancing the ability to provide lethal targeting.

The legal structure and processes guiding this capability appear to have lagged behind RPA use and are admittedly frustrating for American policymakers and strategists. "I think creating a legal structure, processes, with oversight checks on how we use unmanned weapons is going to be a challenge for me and for my successors for some time to come," President Obama stated.[40] In the absence of other prevailing guidance, the enemy has an opportunity to occupy the policy vacuum and exploit the same advancements in technology to stage attacks against US interests abroad. Though the war in Iraq is technically over, political reverberations continue. Additionally, forces remain in Afghanistan where the enemy remains both resilient and resurgent. As such, the current conflicts remain irregular in nature and provide ample opportunity for attacks by RPAs that have, over a long course of time, begun making impacts on the character of war. The role that small-scale assets will play is evolving quickly as well.

Small-Scale RPAs in an Irregular Context

Instead of ferrying passengers or cargo, unmanned aircraft ferry intentions: the intent to view, to monitor, to witness, to surveil, and if necessary or desirable, to attack. And while the most common RPAs reside in the full-size spectrum of platforms (Reaper, Global Hawk, Sentinel, Predator, etc.), technology is opening the door to smaller and less-expensive models to accomplish the same or similar effects.

Traditionally, the use of RPAs was limited to state actors with an established defense sector and corresponding budget – it is an expensive technology. But as this technology advances and cheaper models are available through commercial hobby platforms or boutique production methods, the ability to ferry hostile intentions is created for a fraction of the cost and a portion of the size. In short, there is a risk that malicious use of

[39] Bowden, "Predator Drone"
[40] Bowden, "Predator Drone"

small-scale RPAs will go mainstream. As Colin Gray argues, "enemies of America who cannot afford to emulate US investment in, say, space systems, long range air power, or networked communications, will be obliged to pursue Brodie's logic and seek strategic behavior that works well enough, be it ever so inelegant and probably decidedly irregular."[41]

The use of small-scale RPAs in irregular warfare is a tempting asset if you seek to inflict damage at an acceptable price point. The tools required for a small-scale RPA attack are not only available, but are also inexpensive and provide precision-attack capabilities, minimizing waste and error in an attack. As illustrated in previous chapters, air bases are vulnerable to attack, though it is rare that attacks seek an overthrow of the installation. Instead, most air base attacks are standoff in nature and seek to disrupt and harass the incumbent's ability to project power. As technology increases and the cost of standoff methods of attack decrease, there exists an opportunity to employ small-scale RPAs as effective precision-delivery mechanisms.

The economic benefits of globalization means there is an unprecedented openness on the market, offering previously unavailable resources to the masses. For example, the Internet, cellphones, satellite communications, electronic funds transfers, and ease of international movements and trade are all commonly recognized benefits.[42] Globalization has also "prompted the proliferation of low-cost, high-lethality individual weapons systems like assault rifles, portable antiaircraft missiles, rocket launchers, mines, and extremely powerful blast munitions such as thermobarics."[43] Ultimately, the ease by which information and resources can now change hand means a menu of hostile options exists for an enterprising enemy seeking harm to the US and its associated resources. At their disposal rests a low-cost, high-lethality opportunity for attack.

Enemy forces using this tactic are not likely to harbor delusions of grandeur, expecting strategic results from harassing attacks. There is, however, psychological value worth exploiting. When the 1915 raids on London took place, the fight essentially

[41] Keith L. Shimko, *The Iraq Wars and America's Military Revolution* (New York, NY: Cambridge University Press, 2010), 42.
[42] David Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (New York: Oxford University Press, 2011, 2009), 9.
[43] Kilcullen, 9.

came to the English in ways they could not prevent. If current doctrine creates gaps and seams in the battlefield and leaves the Air Force largely to itself for defense, will the platforms apportioned for air base defense adequately defeat a small-scale RPA attack? First, it has to be assumed that the damage of such an attack warrants prevention. In other words, is the risk of this type of attack sufficient for US policymakers and commanders to take preventive action toward mitigating the threat?

Perhaps the risk of this technique is acceptable in the grand scheme. After calculating the odds of this method being used, the likelihood of it being used successfully, and the risk of intolerable damage occurring, perhaps the answer will suggest it is safer to focus resources on other areas of the fight than to defend against these attacks. However, if a successful volley of attacks renders a $200-million-dollar aircraft incapable of flight through $500 of hobby-like equipment and small explosives, the risk may become relevant. If so, how will the Air Force defend against a 35lb remote-controlled asset made from mail-order parts and common-access chemicals and munitions?

Using an A-10, F-16, F/A-22 or similar is a gross over-match in capability, however it may be possible to employ these aircraft for base defense, given they are mission-ready, paired to a crew and appropriately armed in advance. An initial review of capabilities at the unclassified level shows that these aircraft may be capable of defending an air base against such an attack.[44] The concern, however, is collateral damage to the very base it seeks to protect. Given that small-scale RPA attacks will launch within the base security zone, any subsequent intercept with look-down/shoot-down capability means the people and equipment of the airfield lie beyond or under the path of any interceptor's bullets. To pose a metaphor, it is akin to using a sports car to chase a honeybee, but the honeybee is in your own yard and the sports car has to avoid fratricidal damage in the chase. Perhaps the best defense is one that prevents the honeybee from gaining access in the beginning.

Small-Scale RPAs in Terrorism

In *How Terrorism Ends,* Audrey Kurth Cronin makes a strong argument about

[44] Does this imply a more effective classified capability exists? The author intentionally limited research to open-source capabilities and is unaware if better technology exists. Further, it is beyond the scope and authority of this thesis to explore classified information.

greater access and its effect for terrorism. Terrorism's perceived success "was linked to greater access to more lethal means of destruction. Technological advances, particularly in the increasing sophistication and potency of explosives, seemed to favor the use of terrorist violence in the twentieth century. Although there were fewer attacks overall in the 1990s than there were in the 1980s, the average number of casualties per incident grew."[45] Kurth Cronin later reveals that radical Islamist terrorism is a serious threat, not just because it can kill significant numbers of civilians, but also because "it has the potential to evolve into a broader systemic war that can further change states and even reshape the nature of the state system."[46]

This thesis does not suggest that the use of small-scale RPAs by terrorists will result in an overthrow of the state system. Nor would Kurth Cronin likely suggest the same. Instead, small-scale RPAs are a tool that can be used to detrimental effects if properly employed in both the physical and psychological sense. Expeditionary locations pose a much more focused and niche target set for an adversary. Without large populations of Americans or American infrastructure, the use of weaponized small-scale RPAs is not likely to yield stateside protests capable of unseating our government structure. There is a larger potential, however, that if small-scale precision attacks take place in the homeland against US infrastructure (such as airports, railways, reservoirs, power stations, etc.) or civic facilities (such as school playgrounds, churches, outdoor concerts, sports arenas, marathon finish lines, etc.), the attacks will yield the psychological damage to disrupt and panic daily life momentarily.

It is not as likely that a non-state adversary will seek to overthrow the US entirely, but merely make political and ideological statements expressing its ability to exploit American weaknesses and dependencies. Kurth Cronin captures this with her conceptual framework for three strategic actors in a kind of terrorist triad: the group, the government, and the audience. Specifically, the elements represents the group using terrorism to achieve an objective, the government being targeted by their attacks, and the audience(s) influenced by these acts of violence.[47]

---

[45] Audrey Kurth Cronin, *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns* (Princeton, N.J.: Princeton University Press, 2011), 5.
[46] Kurth Cronin, 6.
[47] Kurth Cronin, 6-8

In the scenario of a small-scale RPA attack overseas, the military installation may represent the government element of the triad, but only loosely as it is not as likely to cause the disruption or unseating of government as previously mentioned. An attack on a military base is not the same as an attack on the Capitol Building or White House, for example. Further, even the audience is slightly distanced. Americans understand the role of the military as the fighting arm of our nation's political aims, though not all are likely familiar of the Clausewitzian axiom of war as an extension of politics by other means. All the same, Americans understand that the military is the embodiment of legitimate violence for the United States and may understand that the likelihood for casualties exists. Despite any aversion to American casualties, the social contract between the fighting Airman and the stateside American is one of implied understanding: we will fight so you do not have to.

Tying this back to Kurth Cronin's triad means that the message sent by terrorists on overseas attacks might not leverage the same effect as one against Americans in the homeland. This distance between Americans and their military forces (both physically and socially) means the audience of the triad is less likely to suffer or feel the effects of an attack, especially if the attack targets a military installation. An attack on a civil landmark or other non-combatant structure would assuredly provoke American interest and concern more than a similar attack on an overseas military post. This is not because Americans feel less compassion for their armed forces, but rather responds to the social contract previously mentioned. The armed forces are lawful combatants and targets; an attack against them may be seen as distasteful, but at a raw level of understanding it is also the cost of doing business.

Lastly, the remaining element of the triad is the terrorist group itself. With the availability of off-the-shelf technology capable of executing an attack, the question to ponder is if a select group of already-established terrorist organizations will adopt the technology, or if it will be used in more diffuse ways, empowering smaller and less-established units. This boils down to a group's stated desire to exact violence and reap the benefits of doing so. There is a communicative element behind violence, and attacks can be as much about destroying infrastructure and machines of war as they can be sending a message. "In short, violence is intended to shape the behavior of a targeted

audience by altering the expected value of particular actions. Put otherwise, violence performs a communicative function with a clear deterrent dimension."[48]

The proclivity to enact violence then becomes an issue for consideration. According to some international relations theorists, it is not likely that most violent intentions will manifest. To this end, small-scale RPA attacks may not align with reality. For example, Stathis Kalyvas elaborates:

> Fantasies of revenge for all kinds of petty everyday conflicts appear to be widespread across all eras and societies, but they are rarely enacted – even less enacted in a homicidal fashion. Thomas Schelling notes that there must be a million people living within the public transportation radius of his home who could burn down his house with impunity and a dollar's worth of gasoline, or could kidnap his children as they played in the street, and, although he would be willing to pay much to forestall such easily accomplished damage, he is puzzled by the fact that he has never been targeted. Whether it is due, as Schelling claims, to the difficulty of translating this action into concrete benefits, to internal moral restraints, to fear of sanctions, or just to stupidity or smallness of soul as Friedrich Nietzche argued, the fact remains that there is a surprising scarcity of violence relative to its actual desire and a pronounced discrepancy between vengeful desires and vengeful acts.[49]

While Schelling's analogy is poignant and he is curious about why such an act has not happened, it does not at all mean that other heinous acts of violence are absent. Attacks of that nature are a truism of terror. For example, in 1995, the Aum Shinrikyo cult killed twelve people and injured over one thousand others when they released 159 ounces (just under ten pounds) of deadly sarin nerve agent on three Tokyo subway trains.[50] Mass panic resulted from the attack. In their planning, the group attempted to spray the chemicals from the air, using remote-controlled helicopters which crashed during testing.[51]

From an attribution standpoint, it is far less likely that a state actor would choose this type of attack on US soil, and to a certain extent, against US forces abroad. It is

---

[48] Stathis N. Kalyvas, *The Logic of Violence in Civil War*, Cambridge Studies in Comparative Politics (Cambridge: Cambridge University Press, 2006), 26.
[49] Kalyvas, 337-338.
[50] David E. Hoffman, *The Dead Hand: The Untold Story of the Cold War Arms Race and Its Dangerous Legacy* (New York: Anchor Books, 2010), 482.
[51] Eugene Miasnikov "Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects", *Center for Arms Control, Energy and Environmental Studies, Moscow Institute of Physics and Technology* (2005): 25.

more likely that terrorist organizations or their respective non-state proxies could employ such tactics. Security assessments of the operating area must consider the possibility of small-scale RPAs as a distribution platform for nerve agents or other toxic materials, especially in an irregular-war context where terrorism is common.

Small-Scale RPAs on the Outcome of War

"Advancing technology makes war more horrible and presumably increases the desire for peace; the very rapidity of the advance makes for uncertainty in everyone's planning and destroys the possibility of an accurate estimate of the likely opposing forces. Each major advance in the technology of war has found its prophet ready to proclaim that war is no longer possible: Alfred Nobel and dynamite, for example, or Benjamin Franklin and the lighter-than-air balloon."[52] This thesis does not pretend that RPAs or their small-scale siblings represent a game-changing technology with regard to achieving peace more quickly. The small-scale RPA is one more iteration of an already-existing technology and is simply evolutionary versus revolutionary in its application.

Does that mean it should be discounted as a viable means of inflicting violence and harm, however? No, not entirely. Instead, strategists should understand this technology is merely a tool available to those wishing to do us harm, much like smokeless gun powder, rifled barrels, and the internal combustion engine helped shape the character of war in past decades. Coupled with a more comprehensive strategy, an adversary can use this tool as a means to accomplish greater objectives or effects on the battlefield. In the current context, the adversary most likely to employ such a technology is irregular in nature.

In other words, this technology will not likely hasten peace if used against us by an adversary, but may complicate our ability to execute our own objectives that seek a peace according to our terms. The goal remains a better state of peace after a conflict; it is not likely this technology empowers an adversary sufficiently to undermine our own efforts and our ability to gain the peace we seek. Instead, using this technology will likely continue to fall under the parameter of pestilence or harassment, with the goal being an

[52] Kenneth N. Waltz, *Man, the State, and War: A Theoretical Analysis* (New York: Columbia University Press, 2001), 235.

interruption of our ability to project power. In that absence of power projection, the enemy seeks a foothold. Without greater means than harassing attacks, that foothold is likely tenuous and temporary. The concern becomes the costs we are willing to accept in this exchange.

In, *Airpower and the Ground War in Vietnam,"* Donald Mrozek states, "Technical proficiency, operational effectiveness and technological capabilities do not suffice in war. Without a strategic vision that turns out to be the right one (or a right one), these become phantom victories leading to a final spectacle of defeat or stalemate."[53] This is an accurate assessment. While an enemy (especially in an irregular warfare context) would prefer to defeat the US, it knows it will take a long time in a protracted war. Small-scale RPAs are a cost-effective means of delivering the harassing attacks which aim to erode their adversary's will by denying it the force-on-force battle which we are organized, trained, and equipped to fight. Additionally, these assets offer an acceptable price-point for commercially available and expendable resources to accomplish their desires, even if the desires do not immediately seem linked to an overarching strategy. This is not to say there is an absence of a strategy, but if one exists, it is more likely a punishment form of coercion.[54]

[53] Donald J. Mrozek, *Airpower and the Ground War in Vietnam* (Maxwell Air Force Base: Air University Press, 1988), 157.
[54] Stephen Chiabotti, School of Advanced Air and Space Studies, feedback with author.

Chapter 5

SMALL-SCALE RPAs: CAPABILITY, INTENT, DEFENSE AGAINST, AND CONTRIBUTING FACTORS

Introduction

The argument for small-scale RPAs as a threat to US air bases rests upon multiple premises. First, air bases are an important aspect of power projection, and history reveals they repeatedly suffer standoff attacks. These attacks rarely seek to conquer or defeat an airfield, but instead aim to disrupt sortie generation and, by extension, power-projection capability. By continually harassing an airfield in this fashion, the adversary is capable of weakening US resolve without encountering unacceptable losses of its own forces in the process.

Second, the US is historically poor at countering standoff attacks against air bases. This is exacerbated by a shift from Cold War air-base-defense doctrine to methods required for irregular warfare. Namely, by addressing the isolated, population-centric character of irregular warfare, doctrine no longer uses manpower-intensive means to establish large front and rear areas of security, which buffer an air base from enemy forces. Current doctrine focuses on mobility and maneuver to secure isolated areas of resistance. While it justly addresses Army objectives, it endangers airfields by creating seams in the battlefield which ease enemy encroachment. This encroachment facilitates standoff attacks by allowing an enemy to stage operations in close proximity to the air base. Under old doctrine that established front and rear areas of security, the base was historically more isolated, making a standoff attack more difficult and risky. Current adversaries understand the value of an air base for power projection and their potential vulnerabilities. Instead of fighting US air power head-on, they attempt to blunt its effectiveness by interrupting air base operations through irregular means and standoff attacks on air bases themselves.

Third, small-scale RPAs are an effective tool to conduct attacks against an air base because they offer affordable means of executing attacks with precision. As air power developed over time, theorists simultaneously conceptualized applications for RPAs. In theory, RPAs would allow a user to gain air power benefits without the traditional air

power price tags. In reality, most of the early RPA attempts failed because of technological shortfalls. Over the coming decades, however, technology advanced considerably, effectively turning RPA theories into reality and catapulting the ability to extend air power over the horizon without consequent risk to the pilot. Through these advancements, platforms grew in capability while decreasing in size. The affordability, capability, and growing lethality of RPAs began to trickle down into small-scale iterations. By making lethality available at such small costs and without considerable logistics-support requirements, small-scale RPAs became an effective tool for precision standoff attacks.

This chapter builds upon historical RPA theories and applications by illustrating the prominence of real-world, off-the-shelf capability arising from RPA market growth. There is an alarming ease with which adversaries can use open-market, commercial options to build and deploy small-scale RPAs as precision standoff weapons. Commercial market growth creates a demand for the use of small-scale RPAs for military and civil applications, which in turn, leads to increased technology that provides enhanced RPA capability at a decreased cost. Further, as capability and affordability advance, ease of use increases. These factors combine to provide an effective and affordable precision standoff weapon on the open market. With this capability, attacks become feasible against the US and its allies as well as their military and civilian infrastructure.

Bureaucratic challenges in US and international policy exacerbate the threat and increase the ease by which these platforms can be used maliciously. For example, in the US, current RPA policy focuses largely on issues relating to Fourth Amendment privacy concerns and the integration of large-scale RPAs into the national airspace. As such, the threat of small-scale RPAs and hobby-modified variants often goes overlooked. Further, the hobby-aircraft market experienced notable growth over the past several years, meaning the capability to hone skills for an attack often goes unnoticed and is, in many cases, perfectly legal. The US is not alone in this regard; research in Russia in 2005

identified the most likely terrorist threat faced by Russians was self-made mini-RPAs stemming from model aircraft.[1]

If small-scale RPAs are to pass from theory into a realistic method of attack, their success depends on the following factors: capability (e.g. platform and payload; communication and navigation of the actors), intent, and physical defense against the attack. Other factors complicate prevention and contribute to the threat, such as market growth signaling a rise in popularity of unmanned vehicles that make an attack attractive, and policy challenges that offer loopholes by which an attack might be mounted. The US must act decisively and intelligently if it is to exploit a technological advancement for its own good while simultaneously denying such privilege to the enemy.

Capability: Platform and Payload

In a 2012 conversation, officials at USNORTHCOM stated that a small-scale RPA attack against the US homeland was unlikely due to the high cost, low payload capability, and line-of-sight limitations of most open-market platforms.[2] While that inquiry focused specifically on an attack against stateside US air bases, it is the answer that is most revealing. From at least 2005, the capability to conduct small-scale RPA attacks against stationary targets appears entirely feasible. To claim in 2012 that such limitations still exist is surprising; denying such a capability and threat exists appears unnecessarily dismissive.

For example, in April 2000, the Yamaha Motor Company used their RMAX industrial-use unmanned helicopter to observe the Mt. Usu eruption in Hokkaido, Japan. This was particularly noteworthy as the RMAX flight was equipped with a GPS flight control system, making it the first case in the world of a successful helicopter operation outside visual range with GPS autonomous flight controls.[3] The RMAX is an autonomous agricultural sprayer that is considerably smaller than manned crop-dusting aircraft. It has a length of 108in, width of 28in, and can carry 61 pounds of liquid

[1] Eugene Miasnikov "Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects", *Center for Arms Control, Energy and Environmental Studies, Moscow Institute of Physics and Technology* (2005): 23.
[2] Emails with the author in 2012. Officials requested anonymity in citing them as a source.
[3] "RMAX Type IIg/Type II History," Yamaha RMAX History, April 8, 2014, accessed April 15, 2014, http://rmax.yamaha-motor.com.au/history.

payload dispersed in less than six minutes.[4] The RMAX represents the leading edge of autonomous unmanned systems, and its performance makes it an appealing platform for military applications. Although Yamaha claims the RMAX cannot be used for military applications because it becomes inoperable beyond radio range, the Mt. Usu eruption indicates its features are easily modified for autonomous missions.[5] Despite the company's insistence that it cannot be used militarily, Yamaha was accused in 2006 of selling the RMAX to a Chinese technology company with ties to the People's Liberation Army, violating Japan's Foreign Exchange and Foreign Trade Control Law.[6] Yamaha claims that approximately 2,400 RMAX helicopters currently fly in Japan, representing 77% of the market share.[7] Acquiring an RMAX is unlikely; however, borrowing from its open-source technology may be less problematic.

Other platforms in use internationally demonstrate how the respective capabilities exist to be payload-bearing, small-scale platforms that can provide standoff range. These models, found below in Table 1, include the Italian CORVO, Singaporean SKYBLADE II and III, United States RAVEN, and the Australian MANTIS.[8]

[4] "RMAX Type IIg/Type II History," Yamaha RMAX History.
[5] Patrick Miller, "Mini, Micro, and Swarming Unmanned Aerial Vehicles: A Baseline Study", *Library of Congress* (November 2006): 29. Miller quotes Tomohiko Otsuka, "Yamaha Unmanned Helicopters Can Easily Be Converted to Military Use; Company Oblivious About Military Value," *Tokyo Sankei Shimbun,* Aug 6, 2006 (via Open Source Center JPP20060807036001).
[6] Miller, 29.
[7] Author Unknown, "Rmax Type IIG/Type II History"
[8] Miller, 31-45.

Table 1. Small-Scale RPAs by Country and Model
Source: Patrick Miller, "Mini, Micro, and Swarming Unmanned Aerial Vehicles: A Baseline Study", Library of Congress *(November 2006): 31-45*

Platform	Country	Size	Payload	Performance	Other
CORVO	Italy	6' wingspan, 17lb MTOW	15lb	222km/h, 8hr endurance, 2000' ceiling	3 levels of navigation: non/semi/fully autonomous
SKYBLADE II & III	Singapore	6' wingspan	N/A	129km/h, 2hr endurance, 4500' ceiling	Autonomous nav, battery and piston-powered
RAVEN	United States	4' wingspan, 4lbs MTOW	0.5lb	96km/h, 2hr endurance, 10km radius	GPS, auto navigation
MANTIS	Australia	5' rotor, 17lb MTOW	.16lb	18 minute endurance	Based on hobby aircraft

Capability: Communication and Navigation

Currently, the less-costly platforms are hobby versions and as such are line-of-sight limited due to the control transmitter. Additionally, flying in crowded areas or between large buildings such as urban canyons subjects many remote-controlled aircraft to radio-frequency interference. This could be a significant hindrance for a user attempting to fly a small-scale RPA in a downtown area, as the surrounding buildings and limited line of sight will impede the effective control and range of the RPA. This is less likely a concern in expeditionary locations, however, as the area surrounding the airfield must be free of obstructions to the maximum extent feasible for safety of flight. While this provides the operator with better line of sight, the same visibility potentially opens the user to discovery.

For these reasons, range and autonomy becomes the friend of a user since these traits provide greater standoff protection. While this standoff may have been a significant challenge in the past, current technology enhances communications with the RPA over long distances and beyond line-of-sight. Small-scale RPAs and hobby variants increasingly incorporate GPS, payload capabilities and motion-capture video for just a

few hundred dollars. For a few thousand dollars, models exist that have real-time video feeds and a payload up to twenty pounds. This provides the potential precision and lethality required to interrupt airfield operations if the attack successfully targets vulnerable areas.

Precision navigation, though possible, is still a significant challenge. As with the other performance parameters, however, technology eases this obstacle. The hardware, software, and instructions to augment less expensive hobby platforms are increasingly available online. For example, in 2006, a Massachusetts resident provided step-by-step instructions on equipping a commercially available radio-controlled aircraft with a Garmin ForeRunner wristband GPS unit. Using computer freeware and open-source satellite overlays (provided free at the time for Massachusetts residents), the user integrated a waypoint-navigated sortie assisted by topographical data for approximately $170 plus the cost of the aircraft.[9]

Other systems exist that do not require hacking or adaptation like the Garmin ForeRunner example. UTC Aerospace Systems offers the Piccolo family of autopilot systems as part of their Cloud Cap technology program. The Piccolo Nano is, "designed to meet the requirements of the smallest UAVs where the vehicle structure provides the enclosure and the autopilot components need to be distributed within the airframe's available space."[10] The Nano is amazingly capable in view of its diminutive size: a 1.8x3.0 inch system provides avionics, 900 Mhz radio and capability for 12 GPS waypoints at only 0.14 pounds[11] – only slightly heavier than a chicken egg.

Within the Piccolo family is the SL model of autopilot system. Larger than the Nano but more capable, the SL avionics system includes a flight-control processor, inertial sensors, air-data sensors, GPS receiver and datalink radio in an enclosure protecting against electromagnetic interference.[12] This model accepts up to 1000 GPS

[9] "GPS Equipped Radio Controlled Sailplane HOWTO," February, 2014, accessed April 12, 2014, http://jeklink.net/projects/GPS_Equipped_Radio_Controlled_Sailplane.html).
[10] Data sheet for Piccolo Nano, "Piccolo Autopilots: The Standard in UAS Systems," Cloud Cap Technology, April 13, 2014, accessed April 13, 2014, http://www.cloudcaptech.com/piccolo_system.shtm.
[11] Data sheet for Piccolo Nano
[12] Data Sheet for Piccolo SL, "Piccolo Autopilots: The Standard in UAS Systems," Cloud Cap Technology, January 2014, accessed April 13, 2014, http://www.cloudcaptech.com/piccolo_system.shtm.

waypoints for autopilot and has the capability for two centimeter digital GPS auto-land and precision-hover helicopter applications. At approximately 5x2x1 inch in size, it weighs 110 grams, or about a quarter of a pound. [13] Putting this in context, an RPA using this system could navigate to any of more than 1000 waypoints and hover above a designated target to deliver a precision-guided attack.

A Russian report in 2005 identified the AP50 autopilot system by UAV Flight Systems, Inc.[14] This particular unit stabilized an RPA using integrated roll, pitch, and yaw gyros, a two-axis accelerometer and other systems in conjunction with GPS-derived speed and altitude information.[15] One particularly useful advantage of the AP50 was the ability to fly beyond direct visual range and conduct auto-land functions.[16] The AP50 was roughly the same weight as the Piccolo Nano, and listed at $2700 without power source. The AP50 is no longer in production, but was entirely functional in 2004; a full decade of technological progression means greater capability than the AP50, presumably at the same or better price.[17] At a macro level perspective, 145 autopilot and inertial navigation systems appear in the UAS Yearbook, though not all are suitable for small-scale RPAs or were in service in 2010.[18] This means multiple options exist for the informed buyer. Additional information is in a 2007 publication providing a survey of

[13] Data sheet for Piccolo SL
[14] Eugene Miasnikov "Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects", *Center for Arms Control, Energy and Environmental Studies, Moscow Institute of Physics and Technology* (2005): 18.
[15] Data sheet, AP50. Author Unknown, "UAV Flight Systems Autopilot Products," April 15, 2014, accessed April 15, 2014, http://www.chinaga.com/bank/896.pdf.
[16] Miasnikov, 19.
[17] UAV Flight Systems underwent significant corporate restructuring and is Vesta Technologies today, though it maintains ties to UAV Flight in heritage only; the two are no longer considered associated. Vesta Technologies received recognition from the FBI for its role in combating terrorism after Masoud Khan attempted to purchase its RPA autopilot and video surveillance systems for remote-controlled aircraft in 2004. Khan and his associates were indicted on multiple charges including (but not limited to) conspiracy to levy war against the United States, conspiracy to contribute services to the Taliban, and conspiracy to contribute material support to Laskar-e-Taiba ("LET"). See www.vestatech.com and US v Masoud Khan, et al, Criminal No. 03-296-A, US District Court for the Eastern District of Virginia, http://www.vaed.uscourts.gov/notablecases/kahn/, accessed 15 April 2014.
[18] *Unmanned Aircraft Systems: Global Perspective*, 8th ed. (Paris, Fr: Blyenburgh & Co., 2011), 205-6.

autopilot systems for small fixed-wing unmanned platforms.[19] The report details the off-the-shelf autopilot products and remarks on the future development of these systems.

Ultimately, the intent of providing this survey of technical information is to demonstrate the plethora of technology on the commercial market that demonstrates incredible capability over a decade ago. If the concept of Moore's Law applies to the technology used in small-scale RPAs, then the landscape of platforms will continue to undergo significant advancement every few years. Not only will the guidance and communications continue to advance, but the composition and design of the aerial vehicle will also advance, providing lighter, stronger, more navigable platforms with increasing lethality at a decreasing price. This will remain a vexing challenge as the intent to use these systems maliciously is not without historical precedent.

Intent

Merely being capable of an act does not sufficiently guarantee it will happen. Schelling referenced the ability of evil people to kidnap his children or burn down his house with impunity and some gasoline. The arresting factor between this act taking place or being a figment of imagination is intent. Without intent, the actions we fear most remain as fears, never becoming reality. As evidenced, there exists a menu of off-the-shelf technologies available for small-scale RPAs to be used maliciously; the truly worrisome consideration, then, is the intent to act upon malicious ideologies. Skeptics may dismiss the likelihood of such intent manifesting in an RPA attack, however headlines from the past several years suggest otherwise.

In the summer of 2002, Maynard Hill designed and built the TAM-5, an 11-pound remote-controlled aircraft. Hill defied the odds and sceptics by successfully launching his aircraft on a successful trans-Atlantic flight from Canada to Ireland (3,000 kilometers away) using an automatic flight control system and only three quarts of fuel. The flight lasted 38 hours and 53 minutes, setting world records for the longest distance and longest

[19] *International Conference on Mechatronics and Automation, 2007: ICMA 2007; 5 - 8 Aug. 2007, Harbin, China* (Piscataway, NJ: IEEE Service Center, 2007), Abstract, accessed April 15, 2014, http://ieeexplore.ieee.org/servlet/opac?punumber=4303487.

time flown by a model aircraft.[20] In a poetic affront to those claiming the technology is too complicated for common use, Hill was 77 years old at the time, legally blind, and mostly deaf.[21] Though Hill's adventure was an entirely benign use of available technology, it makes a poignant statement about the ability to adapt common materials for an extraordinary purpose: range may no longer be an issue.

On July 5, 2003, the Tushino airfield near Moscow hosted a rock concert where two female suicide bombers wore "Shaheed belts" consisting of explosives and fragmentary items such as metal balls and screws.[22] One bomb failed to detonate as designed and killed only the bomber. The second, however, exploded among a crowd of people standing in line at the ticket office, killing 15 and injuring over fifty.[23] Had the same bomb been air-released a few meters above the crowd, the dispersal geometry would have varied significantly, drastically increasing the number of victims by avoiding the human shield phenomenon of those closest to the bomber (which potentially saved many more lives).[24] In other words, the use of an RPA in this instance could have proven far more lethal.

In 2006, authorities convicted Maryland schoolteacher Ali Asad Chandia after trying to acquire a model aircraft autopilot system on behalf of the Pakistani terror group, Lashkar-e-Taiba. This configuration enables an aircraft to receive GPS coordinates and activate a video camera over desired locations.[25] Similarly, Christopher Paul of Columbus, Ohio was accused of joining Al Qaeda in the early 1990s. In 2008, he pled guilty to planning terrorist attacks in the US and Europe and claims he performed research on remote-controlled models, including a boat and a 5-foot long helicopter.[26] In September 2011, Rezwan Ferdaus, a Northeastern University graduate with a degree in

---

[20] Miasnikov, 13. For more, see Emily Sohn, "Model Airplane Flies the Atlantic," Student Science, December 15, 2003, accessed April 17, 2014, https://student.societyforscience.org/article/model-plane-flies-atlantic.
[21] Sohn, "Model Airplane Flies the Atlantic,"
[22] Miasnikov, 8. In this example, Miasnikov specifically references the increased damage had the attack come from an RPA.
[23] Miasnikov, 8.
[24] Miasnikov, 8.
[25] Kelsey Atherton, "Senate Hearing: Drones Are 'Basically Flying Smartphones'," *Popular Science*, 21 March 2013, 1, accessed April 16, 2014,http://www.popsci.com/technology/article/2013-03/how-drone-smartphone.
[26] Atherton, "Senate Hearing: Drones Are 'Basically Flying Smartphones'"

physics, attempted to pilot a large remote-controlled aircraft filled with C-4 explosives into the Pentagon and US Capitol. An FBI sting and subsequent arrest prevented Ferdaus' from carrying through with the operation.[27] The Boston Marathon bombings on April 15, 2013 demonstrated the relative ease by which terrorists target large crowds, achieving substantial psychological impact absent a substantial number of deaths. The very nature of the air domain allows the bypassing of ground-based obstacles. It merits considering if the Boston Marathon attack could have been done as an airborne IED with payload-bearing small-scale RPAs, and, like the Moscow concert, the results could have been far worse.

In March 1985, terrorists used an improvised system of parts to construct a 9-barelled mortar in an attack upon a police station in Newry, County Down, Ireland. Of the nine mortars launched, three were duds, two exploded mid-air, and three overshot the target, but the ninth hit a canteen, killing nine off-duty police officers.[28] The projectiles from the cannon came from adapted oxygen cylinders packed with 44lbs of explosives each and fitted with rudimentary fins. The cannon was loaded onto a truck, parked about 220 yards away and detonated with a delayed timer device that gave the terrorists time to escape. The explosives, electronic components, and remote-controlled detonation system came from parts commercially available in Northern Ireland at the time.[29]

The Newry attack illustrates two relevant issues. First, terrorists "have never been slow to utilize advanced technology weapons and equipment for their own ends, although they are normally forced to adapt available technology rather than having sophisticated equipment developed specifically for their needs."[30] Second, the Provisional Wing of the IRA used commercially available devices, meaning that, although inaccurate, the IRA did not have to risk smuggling in the required bits and pieces vital to the attack.[31] These reasons align with the findings of a report compiled by the Library of Congress, stating

---

[27] Paul Cruickshank and Tim Lister, "Analysis: Model Airplanes as Weapons of Terror," *CNN Online*, September 29, 2011, accessed April 16, 2014,http://security.blogs.cnn.com/2011/09/29/analysis-model-planes-as-weapons-of-terror/.
[28] Richard S. Friedman, *Advanced Technology Warfare: A Detailed Study of the Latest Weapons and Techniques for Warfare Today and Into the 21st Century,* American ed. (New York: Harmony Books, 1985), 199.
[29] Friedman, 199.
[30] Friedman, 199.
[31] Friedman, 199.

that terrorists use (in this case, RPAs) "for the same reason that the United States and its allies use UAVs: low cost, simplicity, covertness, and psychological effect.[32] While the Newry attack did not use RPAs, it took place nearly thirty years ago, before such unmanned technology became ubiquitous. The attack did, however, utilize the same fundamental concepts discussed herein: standoff, affordability, simplicity, and commercial componentry.

In a contemporary example, small-scale RPAs made recent headlines when, after a series of artillery barrages from North Korea, officials discovered "toy-like drones" on a South Korean border island.[33] The aircraft were larger variants of platforms displayed the previous year in a military parade in Pyongyang, North Korea, but were not believed to be capable of air strikes or long-range surveillance.[34] Though the North did not overtly claim ownership, Kim Jong-un did claim in state-owned media that he supervised a drill of "super-precision" RPA attacks on a simulated South Korean target.[35] Even if the RPAs represent North Korean rhetoric, there is still a potential threat with aircraft of this nature. These aircraft do not have to be inherently high-tech or a leading-edge-capability product; "This type of toy-like equipment can find a blind spot."[36]

There is a metaphorical value in comparing this technology to cyberspace operations and cyberspace threats. In both cases, overwhelmingly benign civil tools can be used maliciously, but the preponderance of use is much less threatening. It is admittedly challenging to use technology for civil benefits while restricting it in a way which provides the same beneficiaries with security. In other words, the balance between freedom of use and security is delicate. Cyberspace operations, however, benefit from agencies dedicated to defense against cyber exploitation in an attempt to minimize the threat. In the Department of Defense, there is neither a sufficient organizational

---

[32] Patrick Miller, "Mini, Micro, and Swarming Unmanned Aerial Vehicles: A Baseline Study", *Library of Congress* (November 2006): 27..
[33] Reuters, "Drones That Crashed in South Korea 'came from North Korea'," *Telegraph*, April 2, 2014, accessed April 16, 2014, http://www.telegraph.co.uk/news/worldnews/asia/northkorea/10738567/ Drones-that-crashed-in-South-Korea-came-from-North-Korea.html.
[34] Reuters, "Drones That Crashed in South Korea 'came from North Korea'."
[35] Reuters, "Drones That Crashed in South Korea 'came from North Korea'."
[36] Reuters, "Drones That Crashed in South Korea 'came from North Korea'." Here, the article quotes Kim Hyoung-joong, a cyber defense professor at Korea University in Seoul.

perspective dedicated to countering RPAs nor an organization tasked to coordinate the multiple-service approaches.[37] Absent an overarching focus to defend against RPAs, we place at risk our infrastructure, assets and personnel.

Physical Defense

"It is very difficult to stop a terrorist UAV once it is launched."[38] This is an accurate assessment. Further, defending against an attack is challenging due to the ease by which once can convert a readily available radio-controlled hobby aircraft and use it for terrorist activities.[39] While expeditionary installations in hostile areas may have adequate counter-measures available, stateside or overseas permanent bases aren't likely to have active defense capabilities. One significant reason is the need for the US to abide by host-nation sensitivities and status-of-forces agreements. It may be politically untenable, for example, for Ramstein Air Base to have a fully automatic machine gun turret on the fence line to contend with a small-scale RPA attack.

Second, it is difficult for leaders to assess risk and likelihood versus cost. Even if a defensive system or device is allowable by a host nation, the risk of attack may not warrant the expenditure of the defensive system. Gormley refers to this as "unfavorable cost-exchange arithmetic."[40] For example, consider the US missile defense systems and their cost for the purpose of defeating a conceivable missile threat. "The guidance upgrade alone on the PAC-2 Guidance Enhanced Missile costs $400,000 per missile, and each new PAC-3 interceptor costs $3.5M."[41] For a fraction of the cost, an adversary could field several cruise missiles or possibly even converted airplanes, which could saturate most economically feasible missile-defense architectures.[42] There is an

[37] Darin Gaub MAJ, "Unready to Stop Uavs: It's Time to Get Serious About Countering Unmanned Enemy Aircraft", *Armed Forces Journal* 149, no. 5 (December 1, 2011): 1, accessed April 16, 2014, http://www.armedforcesjournal.com/unready-to-stop-uavs/. For an organizational perspective, the US Army's Fires Center of Excellence at Ft. Sill, OK may be a good start. The Counter-UAS program held its first meeting in December 2012 with approximately 120 attendees across the Joint arena. For more, see http://www.uasvision.com/2012/12/18/fires-center-of-excellence-hosted-first-counter-unmanned-aerial-system-coordination-meeting/.
[38] Miasnikov, 19.
[39] Miller, 27.
[40] House, testimony of Dennis M. Gormley, Monterey Institute's Center for Nonproliferations Studies before the Subcommittee on National Security, Emerging Threats, and International Affairs, US House of Representatives Committee on Government Reform, March 9, 2004
[41] House, Gormley testimony
[42] House, Gormley testimony

appropriate colloquialism which asks, Is the juice worth the squeeze? In many cases, it may not be. It is wise, however, to remember the lessons of irregular warfare, which prescribe fighting enemies where they are weak; a lack of standoff protection may invite a standoff attack, especially if the area inside the perimeter contains lucrative targets.

It is not far-fetched to conceive of terrorists or irregular warfare combatants entertaining the notion of attacking with an RPA, especially if cruise missiles or aircraft are not readily available.[43] One survey of terrorist activity accounted for 43 cases involving 14 groups where the actors threatened, developed, or actually used remote-controlled delivery systems for an attack, including Al Qaeda's plans to use remote-controlled aircraft to kill key leadership at the G-8 summit in Genoa, Italy in 2002.[44] Additionally, according to a report in the London Independent newspaper, a British national held at Camp Delta, Guantanamo Bay, Cuba, confessed to cooperating with an Al Qaeda plan for using anthrax and an RPA to attack the British House of Commons.[45]

Small-scale RPAs, specifically mini and micro platforms, have a very small radar cross-section, making them difficult to find, identify, and shoot down. Further, their low altitude and low airspeed complicate the task of detection and, as of a 2006 report, there were no known shoot-downs of small-scale RPAs.[46] Part of this may be that the technology is not commonly used so that opportunities to shoot one down are rare. Also, it is possible that such shoot-downs take place but remain classified, complicating the reporting procedures for open-source research. The physical traits of small-scale RPAs will likely continue to decrease or will remain roughly the same size but grow considerably more efficient. This means future attempts to defend against these platforms will remain troublesome.

---

[43] House, Gormley testimony

[44] House, Gormley testimony. Here, Gormley refers to research conducted by Louis R. Mizell, a private security expert and former US intelligence officer. For more, see Michael Gips, "A Remote Threat," *Security Management Online Archive*, October 2002, 1, accessed April 13, 2014, http://www.securitymanagement.com/library/001324.html.

[45] House, Gormley testimony

[46] Miller, 21. There is a subtle but important distinction in Miller's report, in that no shoot downs of *mini* or *micro* (paraphrased herein as small-scale) aircraft were shot down. In August, 2006 the Israeli Air Force shot down a Hezbollah RPA, however no details on the means used to shoot it down have been divulged. (Miller, 21) Presumably, the Hezbollah RPA was not small-scale.

Contributing Factors: Market Growth and Policy

Proliferation of technology is especially concerning when it gets manipulated from its original intent into a malicious, marketable form. Policy that fails to address those challenges or prevent proliferation compounds the issue. When technology has a footing in civil industrial bases, proliferation is difficult to monitor, assess, predict, and control.[47] The market for RPAs of all sizes grew considerably over the last decade and poses a problem of proliferation for uses not originally intended. The Yamaha RMAX platform is a good example of an agricultural, benign platform that provides an affordable alternative to manned applications but, if manipulated, carries significant malignant potential. Market growth fosters technology that makes current applications more effective and efficient. It is important, therefore, to keep the technology in the right hands, understanding that "right" can be a subjective declaration.

Small-scale RPAs offer an attractive price-point that compounds the challenge of keeping the technology in responsible hands because it is so readily available. So long as small-scale RPAs cost significantly less than large-scale platforms, and cost exponentially less than manned contemporaries, they will remain viable options for niche aviation markets. While small-scale RPAs measure in the thousands of dollars or less per copy, the next generation manned fighter costs hundreds of millions of dollars. This is not to say that small-scale platforms and fifth-generation stealth fighters are on equal footing with regard to capability; quite the contrary. Rather, it asserts that effects-based operations may be achievable with far more affordable assets. This is especially important in the hands of an adversary without the ability to purchase an F/A-22 or F-35. If budget actions focus on the next generation aircraft, then money will continue to be an issue. Although it sounds apocryphal, experts estimate by 2054, the entire DOD budget will be required to purchase a single aircraft. [48]

---

[47] Senate, testimony of Christopher Bolkcom, Analyst in National Defense for the Congressional Research Service before the Senate Governmental Affairs Committee, Subcommittee on International Security, Proliferation, and Federal Services, June 11, 2002.

[48] John Christie, "DOD On a Glidepath to Bankruptcy", *Proceedings Magazine, US Naval Institute* Vol 134/6/1,264 (June 2008), accessed April 10, 2014, http://usni.org/magazines/proceedings/2008-06/dod-glide-path-bankruptcy. Here, Christie refers to information from Norman Augustine, the former head of Lockheed/Martin Corporation. Augustine postulates that if current acquisition practices are not addressed, the US military will cease in relevance as a result of reduced force structure and overbearing costs. "Law XVI: In the year 2054, the entire

Recent estimates report as many as 50 US companies, universities, and government organizations contribute to developing RPAs, constituting over 150 different unmanned aircraft designs.[49] This does not account for the international market, which estimates 4,000 different unmanned aircraft platforms are in current global circulation, though not all of those are small-scale.[50] In all, market growth for the global RPA sector is forecast at $8.35 billion by 2018 with the US and Israel being the largest revenue generators of those countries producing RPAs.[51] While industry growth is not exclusive to the US, it does highlight a responsibility of the US to safeguard its intellectual and industrial technology. There are at least 40 other countries producing RPAs, some of which may not be viewed as US adversaries, per se, but are not closely aligned with the US, politically. These countries include Belarus, Georgia, Pakistan, China, Russia, and Iran, though this list is not exhaustive. The growing use of RPAs by foreign countries – non-allies, in particular – is potentially troublesome as it can negate the technological edge previously obtained by the US and may pose a risk to US interests overseas as the foreign markets proliferate RPA technology.

RPA market growth in the US began with the civil aviation sector. As a note of clarity, this sector includes more than just the major commercial airlines. As the civil market shrank post-9/11, companies investigated the demand for unmanned aircraft as cost-affordable alternatives for their particular market share.[52] Areas of interest for these companies include agriculture, communications, surveillance, traffic control in cities, pipeline and bridge inspections, etc. The prevailing challenge, though, remains US policy. For example, the FAA currently prohibits the use of RPAs in for-profit operations. This includes use by photographers seeking aerial photos of a city or

---

defense budget will purchase just one aircraft. This aircraft will have to be shared by the Air Force and Navy 3.5 days each per week except for Leap Year, when it will be made available to the Marines for the extra day." Norman R. Augustine, *Augustine's Laws*, 6th ed. (Reston, VA: American Institute of Aeronautics and Astronautics, 1997), 107.

[49] *Unmanned Aerial Vehicle (UAV) Market (2013 - 2018)*, June 2013, Abstract. http://www.reportsnreports.com/reports/253291-unmanned-aerial-vehicle-uav-market-2013-2018-.html

[50] *PR Newswire*, Unmanned Aerial Vehicle Market (Uav) Worth $114.7b by 2023, February 13, 2014, 1, accessed April 13, 2014, http://www.prnewswire.com/news-releases/unmanned-aerial-vehicle-market-uav-worth-1147b-by-2023-245370591.html.

[51] *Unmanned Aerial Vehicle (UAV) Market (2013 - 2018)*, June 2013.

[52] Miasnikov, 3.

landscape, private firms contributing to missing person searches, product delivery by Amazon.com and many others.[53] There are significant bureaucratic hurdles associated with enacting legislation that favors or removes limitations on unmanned aviation; market advocates remain active in their attempts to persuade legislative powers but are making little progress.

The current debate on stateside RPA operations focuses almost exclusively on issues relating to Fourth Amendment privacy entitlements and to integrating large RPAs into the national airspace by 2015. This fails to address small-scale platforms as a domestic threat as well as the aspects of proliferation that may affect US interests abroad. Small-scale RPAs are a threat flying beneath the radar, both literally and metaphorically. One Department of Homeland Security official is on record downplaying the threat, asking, "What terrorist is going to have a Reaper?"[54] This line of thinking and others similar to it focus on the threat, but not the proper platform.

The greater threat to the US and its interests at home and abroad is not the large-scale RPA but rather the small-scale variant, due in part to unsolved policy challenges. For example, no lead agent exists within the federal government with statutory responsibility for regulating RPAs. Further, the hobby market is a viable location for much of the technology applied in small-scale RPAs. Apart from voluntarily enacted safety policies, the FAA has no regulations directly relating to hobbyists and the market they use, which provides off-the-shelf capability for malicious actors. The 2012 Reauthorization Act specifically prohibits the FAA from developing any rule or regulation for model aircraft under a specified set of conditions, such as eliminating the need for a hobbyist license.[55] Additional clarifying rules come from a 1981 FAA

---

[53] While aerial photography and the Amazon.com "drone" delivery are more frequently cited examples, the missing persons search raises the question of policy delays unintentionally hampering otherwise benevolent initiatives. See Jack Nicas, "FAA Unswayed by Do-Good Drones," *The Wall Street Journal*, April 6, 2014, 1, accessed April 17, 2014, http://online.wsj.com/news/articles /SB10001424052702303847804579481281535674284.

[54] P.W. Singer, "Will Foreign Drones One Day Attack the U.S.?," *Newsweek*, March 13, 2010, 1, accessed April 17, 2014, http://www.newsweek.com/will-foreign-drones-one-day-attack-us-75331. Singer quotes Jim Tuttle, a Department of Homeland Security official responsible for safeguarding against non-nuclear weapons, referencing the MQ-9 Reaper.

[55] House, testimony of Gerald Dillingham, Director of Physical Infrastructure Issues, Government Accountability Office before the House Homeland Security Subcommittee on Oversight, Investigations and Management Hearing, 19 July 2012. ProQuest database ID 1027377006.

document, Advisory Circular (AC) 91-57, asking hobbyists to avoid noise-sensitive areas like parks, schools, hospitals, and churches.[56] Given that AC-91-57 is over thirty years old and the landscape has changed dramatically, policymakers would be wise to re-examine the issue.

Public records indicate politicians are aware of and are debating the issue, though discussion of the threat seems sporadic. For example, Representative John Mica (R-FL) stated in 2006, "They [RPAs] can carry explosives…even more concern would be carrying small amounts of chemical or biological material."[57] Seven years later in March 2013, a Senate Judiciary hearing discussed the implication of RPAs in the US and Senator Dianne Feinstein (D-CA) inquired if hobbyists could modify drones to carry and use a weapon.[58] While the discourse is encouraging, there are still legitimate challenges to overcome with any legislation addressing RPAs. The Federal Aviation Administration intends to release guidance by 2015 that will specify integration of full-scale RPAs into the national airspace. It remains to be seen if their policies will affect the flight space likely used by small-scale platforms, specifically platforms weighing 55 pounds or less and flying below 400 feet in elevation. Until then, limiting the proliferation of technology, how it is used, and how it is exploited will remain a challenge.

Performance Limitations and Considerations

Previous use of RPAs required a significant logistics-support system because the platforms were large in size and dependent upon other assets commonly used in an airfield. For example, "as long as the RPAs had to be carried under the wings of C-130s, the logistical footprint of the airplane's crew and maintenance structure had to be deployed along with their additional support."[59] Now that there are smaller, more capable platforms that can navigate with GPS, there is less attachment to a logistics tail as was the case with previous iterations. This means there is an increased mobility and

[56] Federal Aviation Administration, "Federal Register: Unmanned Aircraft Operations in the National Airspace System, Docket No. Faa-2006-25714," February 6, 2007, accessed April 17, 2014, http://www.gpo.gov/fdsys/pkg/FR-2007-02-13/html/E7-2402.htm.
[57] Cruickshank and Lister, "Analysis: Model Airplanes as Weapons of Terror"
[58] Atherton, "Drones are Basically Flying Smartphones"
[59] David Mets, "Rpas: Revolution or Retrogression", *Air Force Research Institute Papers*(paper 2010-1, April 2010): 8.

maneuverability of the launch source, which can be a very attractive characteristic to terrorists or combatants in irregular warfare who benefit from additional mobility amongst the population. The operator does not have to be stationary (and by this, presumably detectable); it may be sufficient to launch from the back of a vehicle already under way.

Additionally, the value of being the originator or first-mover with a technology declines over time as others seek to copy your efforts, but do so for much less expense. Pirated technology may deliver cheap ways to overcome the huge advantage the US retains in terms of conventional warfare.[60] "Another downside of being the leader in RPA (or any other major technological development) is that after you have made the investment in time, energy, and money in the new technology, then the rest can take a free ride on your work."[61] For example, the Soviets avoided the "toil and expense" of a Manhattan Project because espionage "was quicker and cheaper."[62] The advantage the US once held with RPAs can now be quickly and cheaply reproduced. This can bestow upon our adversaries the same air power advantages once monopolized by US forces.

Skeptics may view small-scale RPAs as too exotic or too demanding for the results they are likely to achieve. After all, the results must be commensurate with the effort invested.[63] The world, however, is changing quickly and the rapid development of the science and technology used for small-scale RPAs may escape the casual observer or military strategist. This is particularly problematic because the ability to control and deliver a payload to a specific target gets easier each year, and dangerous effects are not "beyond the power of nonprofessionals."[64] So long as the physical capabilities of the platform are met, skill may not be so important. To that extent, the RPA platform's capabilities are discussed below.

A Russian analysis of the problems of light aircraft design reveals the airframe typically accounts for 25% to 40% of the takeoff weight of the airplane.[65] Unique designs may achieve a number below 25%, but in general terms, the lighter the takeoff

[60] Mets, 15.
[61] Mets, 15.
[62] Mets, 15.
[63] Mets, 15.
[64] Miasnikov, 14.
[65] Miasnikov, 15.

weight, the more payload can be accommodated. There is, of course, a concern for structural rigidity, aerodynamics, and airworthiness. For example, an aircraft made of balsa wood (a popular material for hobby aircraft) may dip below the 25% airframe weight criteria but suffer a reduced capability to ferry heavier payloads and may become unstable as a result of the payload. Therefore, the type of material and its strength is a concern for choosing or designing a platform.

Terrorist applications, or even one-time use applications, can bypass the structural-rigidity concerns to a large extent. "The structural strength required for terrorist mini-UAVs could be substantially less. Since terrorist mini-UAVs are intended for a single use, they can be composed of lighter materials that lose strength over time."[66] Said otherwise, a user can opt out of quality materials and structural strength if using the design for a one-time use, such as in a standoff attack. Small-scale RPAs are not considered re-usable platforms and should be viewed as one-time use, expendable assets. Therefore, inexpensive blends of commonplace materials may suffice for flight demands.

Next, if the platform accomplishes the 25% to 40% airframe weight, 60% or more of the vehicle may be designated for payload, navigation, and fuel, dependent upon a proper aircraft design. The payload must not be of a shape, type, or form that obviates aerodynamic properties and makes the overall platform unstable and incapable of flight. Given aerodynamically acceptable properties, a payload of 60% may afford dangerous effects if the payload is a fragmentary grenade dropped above a multi-million dollar fifth generation stealth fighter, an incendiary bomb dropped above fuel storage bladders, or a canister of chemical or biological material dispersed above fielded forces or metropolitan areas. For example, a 2003 simulation by the National Academy of Sciences revealed if just 1.98 pounds (900 grams) of weapons-grade anthrax was released 100 meters upwind of a large US city, 1.5 million people would be infected.[67]

Two pounds is a feasible payload for the platforms of small-scale RPAs available on the open market. Payloads of this weight can be accomplished using either airplanes or multi-blade/multi-rotor helicopter designs. For example, in the summer of 2013, the

[66] Miasnikov, 15.
[67] Miasnikov, 7, citing Lawrence M. Wein, D. L. Craft and E. H. Kaplan, "Emergency Response to Anthrax Attack," Proceedings of the National Academy of Sciences, Vol. 100, No. 7, pp. 4346–4351, April 1, 2003.

OppiKoppi Music Festival in South Africa offered a unique commodity for concertgoers: free airdropped beer. Using an app on their smart phone that provided precise GPS coordinates, customers requested a beer then stood in a designated drop zone. Later, an autonomous, multi-rotor helicopter arrived above the customers and released a parachute-guided cold beer.[68]

In a similarly light-hearted application, Darwin aerospace recently introduced the Burrito Bomber, "the world's first airborne Mexican food delivery system."[69] In this operation, users connect to the Burrito Bomber web application and place an order. The customer's smartphone generates a waypoint file that is compatible with the aircraft navigation system. The waypoint directs the aircraft to the customer's location and uses a common hobbyist bomb-release tool to parachute a burrito delivery tube to the customer's GPS location. Far from a poorly-envisioned fantasy of getting late-night snacks, the Burrito Bomber employs a sophisticated application of open-source products to ferry a respectable payload weight. The Darwin Aerospace team uses a SkyWalker X8 Flying Wing aircraft with the ArduPilot navigation system.[70] The ArduPilot system is an open-source software system used to autopilot and control fixed-wing aircraft and was the winning autopilot code system in the 2012 Outback Challenge UAV contest.[71]

The commercial market is alive and flourishing with technology that greatly enables small-scale RPAs. With little investment and little experience, users can easily gain access to platforms that not only provide entertainment, but provide opportunity. The opportunity to use this technology for fun or for nefarious purposes rests upon the intentions of the user. If the user intends to do harm, the open-market proliferation of the technology and absence of an overarching policy means there is a wide menu of choices available.

---

[68] "Drone Delivers Beer at Oppikoppi," News24.com, August 8, 2013, accessed April 17, 2014, http://www.news24.com/Technology/News/Drone-delivers-beer-at-Oppikoppi-20130808. For more, see multiple videos available at www.YouTube.com, searching for "Oppikoppi Beer Drone"

[69] "Burrito Bomber," Darwin Aerospace, April 17, 2014, accessed April 17, 2014, http://www.darwinaerospace.com/burritobomber.

[70] "Burrito Bomber," Darwin Aerospace

[71] "Arduplane," DIY Drones, April 17, 2014, accessed April 17, 2014, https://code.google.com/p/ardupilot-mega/.

Policymakers and strategists must recognize that with increasing ease, the resources they attempt to safeguard can be threatened by small-scale RPAs. While some debate the effectiveness of small-scale platforms as viable threats, the open-market technology aptly demonstrates the ability to modify these aircraft in a way that can deliver small ordnance payloads with precision. Futher, market growth provides commercial systems of GPS-enabled autopilot and autonomous flight which have, to date, demonstrated impressive performance at reasonable cost and very little weight. The hobby market reflects the growth of military RPAs and now offers an impressive array of technology with which relatively benign aircraft can be turned into weapons. Merely being capable of an act does not sufficiently guarantee it will take place, however, multiple cases highlight individuals who attempted to use small-scale RPAs against the US. In short, the intent to carry out transgressions with small-scale RPA already exists. Given the available technology and the malicious intent to use it, leaders must remain focused on defense against these attacks. The small radar cross-section of these RPAs makes finding, identifying, and stopping incoming threats difficult.

Calling the conglomeration of these factors a "perfect storm" is hyperbole. However, it is difficult to deny the critical elements for an attack exist: commercial ease of access to a platform, sufficient thrust-to-weight ratios to ferry a dangerous payload, GPS-enabled systems for precision delivery, previously-demonstrated intent, all in a package which is difficult to defend against. Integrating these elements successfully can interrupt air base operations and the projection of air power. The threat also poses concerns for defense of the US homeland and its critical infrastructures. Leaders must address this threat accordingly by recognizing its potential, and training and equipping its forces to respond with [preferably] non-lethal but debilitating counter-measures.

Chapter 6

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Recalling lessons learned from the World War I and II interwar years, Overy states, "What combat experience there was during the inter-war period tended to be between enemies of very unequal resources which gave few clues as to how an air war was to be fought between large air powers with a great parity of striking-power."[1] Taken in today's context, this passage illuminates an important consideration for air power strategists, specifically, the impact of unequal resources and how two adversaries will face each other when one side lacks parity. It can easily be argued that today's irregular wars embody this disparity, whereby our adversaries lack the air power capabilities of the US and in this shortfall, they seek to blunt our means by irregular tactics. Current lessons reveal the criticality and vulnerability of air bases and that attacking with affordable precision is no longer the realm of super-powers with world-class air forces. Specifically, the rapid rate of technological advancement increases affordability, utility, and availability of small-scale RPAs creating a cost-effective opportunity for adversaries to exploit the air domain to their advantage and effectively challenge air base defense and the projection of air power.

History has thus far demonstrated several facts regarding air bases, air base defense, and the proliferation of aviation technology. First, air bases are central to the projection of air power and prove highly susceptible to standoff attacks. Rather than seeking to overthrow, seize, or conquer an air base, these attacks instead seek to harass and interrupt. Harassment and interruption halts the momentum of sortie production and therefore, the ability to launch sorties and project power.

Second, the Air Force, while highly capable of inflicting harm or projecting power over great distances, is ill prepared to prevent standoff attacks which occur in the vicinity of the air base. Since the Korean War, no enemy air force has inflicted an attack upon US ground troops because the Air Force continually attains and sustains air superiority.

---

[1] R J. Overy, *The Air War, 1939-1945*, Potomac ed., Cornerstones of Military History (Washington, DC: Potomac Books, Inc., 2005), 9.

There is an admitted shortfall, however, in its ability to secure terrain outside the air base from which ground attacks originate. These attacks are problematic not because they are strictly conducted on the ground, but because they exploit the air domain to their advantage through quiet, passive, and affordable means. Said otherwise, adversaries launch attacks through the air with ground-based technology that is rapidly increasing in affordability, lethality, and precision. Further, conflicting Air Force and Army doctrine fails to secure the immediate areas surrounding an air base, providing adversaries with the opportunity to encroach with sanctuary. These means counter Cold War doctrine by which much of the US military organized, trained, and equipped for full-scale, state-on-state war.

Third, if air bases remain vulnerable and doctrine exacerbates this risk, then a viable method of attack is the use of small-scale RPAs due to their inherent mobility, ease of use, and difficulty of detection. These platforms are expendable, affordable, and effective means to deliver a precision payload against high-value targets central to the Air Force's ability to project power. The relative cost of a small-scale RPA pales in comparison to the damage they can inflict against vulnerable ground targets such as troop concentrations, parked aircraft, bulk fuel bladders, generators, or communications centers.

Fourth, not only is the concept of using small-scale RPAs feasible, the technology which makes them realistically threatening is readily available on the commercial market. This technology grows more affordable and capable every few years, seemingly following the axiom of Moore's Law. Market growth for small-scale RPAs and hobby variants leads to a proliferation of technology, not just in the US, but in the international community, including non-allied countries. Additionally, multiple cases indicate a willingness to use this very technology in malicious forms; from at least 2000 onward, small-scale RPAs and their related technology were sought by terrorist organizations such as Al-Qaeda and Lashkar-e-Taiba as well as by individuals enacting grievances both overseas and inside the US. While previous aerial platforms failed to perform beyond line-of-sight transmitters or control devices, current iterations utilize GPS waypoint-navigated sorties and demonstrate substantial range capabilities. Many platforms now have payload-carrying capability, meaning the challenges of navigation, range, and

precision delivery previously hosted in multi-million dollar aircraft is available on the open market for a few thousand dollars or less.

Finally, this technology is increasingly difficult to defend against, posing challenges not just to military leaders abroad, but to policymakers at home in the US. Small-scale RPAs offer a very small radar cross-section, making target acquisition and shoot-down difficult. While current US aircraft may be capable of defending against this attack, an adequate defense requires their presence and preparation. In other words, against a small, remotely-located FOB without dedicated air support, small-scale RPAs may be an effective means to target precise resources or personnel in an expeditionary environment.

As previously mentioned, calling the conglomeration of these factors a "perfect storm" is hyperbole. However, it is difficult to deny the critical elements for an attack exist: commercial ease of access to a platform, sufficient thrust to weight ratios to ferry a dangerous payload, GPS-enabled systems for precision delivery of that payload, and previously demonstrated intent, all in a package which is difficult to defend against. Combining these elements successfully can interrupt air base operations and the projection of air power. It also poses concerns for defense of the US homeland and its critical infrastructures. Leaders must address this threat accordingly by recognizing the potential of the threat, and training and equipping its forces to respond with [preferably] non-lethal but debilitating counter-measures.

Recommendations

Recommendations for protecting against small-scale RPAs involve a diverse approach of intelligence assessments, actions in policy, and hardware restrictions. First, it is possible that attacks from small-scale RPAs will not manifest in the way this thesis addresses. Although available data indicates otherwise, attacks ultimately boil down to human decisions and human intentions. For an enemy to pursue this path of attack, the results must be commensurate with the effort they put forth and invest.[2] If adversaries determine that these attacks do not yield the results they desire, it is entirely feasible that they will seek alternate methods to enact grievances. In this regard, intelligence estimates of the threat are pivotal; irregular warfare teaches to attack where the enemy is

[2] Mets, 3.

weakest and if our defensive posture against standoff attacks is weak, perhaps the attacks will manifest in other standoff means than small-scale RPAs. This still implies an attack for which quality intelligence may reveal enemy intentions. With that intelligence, defense planners can equip themselves as needed. As the technology increases for small-scale RPAs, so does the ease of attack; leaders must not be dismissive because the method seems exotic or niche.

Should intelligence reveal the threat warrants attention, political and military leadership can address the issue with multiple forms of policy. First, non-proliferation of technology can help stem the advance of the technology associated with small-scale RPAs. The Missile Technology Control Regime (MTCR) and Wassenaar Arrangement pledge to strengthen the efforts which limit how technology falls into the hands of terrorist groups and ordinary individuals.[3] Conditions of the MTCR do not fully address the technology found on the hobby market and can be modified to address this rise of technology. Specifically, small-scale RPAs can be referenced as a variant of cruise missile and limitations can address the navigation mechanisms available on the open market.

Next, current US policy for RPAs is largely dependent upon FAA regulations for the national airspace and full-scale RPAs. This almost entirely excludes small-scale platforms which are rapidly expanding in capability and danger. There is a growing need to enact legislation in this niche airspace and doing so should not prove politically untenable. After stemming its growth and proliferation through the MTCR, policymakers can address the threat at the source and propose restrictions on the technology being manufactured for hobby markets and non-government applications.

For example, any open-market, commercial technology that enables GPS navigation or autonomous flight must incorporate a type of kill switch that prevents the aircraft from a specified airspeed or altitude. Additionally, payload restrictions can dictate that no aircraft be capable of a specified weight payload without an operator's license issued by an appropriate review process. Any platforms that desire greater capability must be

[3] House, Center for Nonproliferation Studies Testimony of Dennis M. Gormley, Monterey Institute's Center for Nonproliferations Studies before the Subcommittee on National Security, Emerging Threats, and International Affairs, US House of Representatives Committee on Government Reform, March 9, 2004

followed with additional review and approval from a government entity. (*which* government entity remains problematic) This is similar to the restrictions placed on firearms, whereby fully automatic weapons require special review and approval for purchase. Politically, gun control remains a highly volatile subject, yet the hobby market is not likely to carry lobbyist influence akin to the National Rifle Association. In simpler terms, there is not a constitutional right to bear arms for the hobby market and restrictions against payload and navigation are not outright bans – they are simply controlling mechanisms which will not likely suffer public outcry so long as there is still modest access to the technology for hobby use.

Next, given that the threat exists and is viable in a given scenario, soft-kill options need assessment. As previously discussed, kinetic defenses with look-down shoot-down radar carry a consequent collateral damage risk for the air base being attacked. If an air base determines that the use of A-10s, F-16s, F/A-22s or otherwise are suboptimal defense mechanisms, then other applications require consideration. For example, in an expeditionary environment, frequency detection devices may aid the detection of an inbound aircraft. If a detection device locates an airborne object operating at 75 mHz, it could effectively jam the signal and prevent encroachment on the air base. There are multiple risks with this approach, however. First, the detection system must search for multiple frequency ranges and be capable of isolating a signal amidst civic "noise". In other words, the system must be capable of distinguishing between an inbound threat and the use of common radios or communication devices needed by civilians which could suffer in the event of jamming.

Next, should such a signal be detected and jammed, the inbound aircraft could become a falling-explosives hazard to the town beneath it and, if armed, cause collateral damage to local residents. Should this happen, it could provide an excellent opportunity for enemy propaganda to declare how US defenses killed innocent locals. A solution may be to ensure air bases offer a sufficient base security zone (BSZ)[4] and intentionally accept an inbound threat. Once inside the BSZ but still sufficiently away from valuable targets, the RPA is jammed and falls safely within the base and away from civilian areas. It is easier to establish an effective buffer zone such as this when opening an airbase since

[4] Refer to chapter 3 for more.

there is greater flexibility in how the base is arranged. For already-established locations overseas and in the US, redefining the perimeter carries highly difficult and expensive political actions for land rezoning and acquisition. Further, many bases cannot afford the luxury of a buffer zone for the entire installation and merely seek adequate protection for flight operations; the areas around base housing, base schools, and the main operating portion of the installation are rarely, if ever, targeted and may directly butt against the perimeter and lack a buffer zone. Without an intelligence estimate that identifies such a threat, taking actions to redefine base perimeters is highly unlikely.

In closing, David Mets provides valuable insight. "Perhaps now the modern equivalent of the medieval knight is an individual jihadist armed with remotely detonated IEDs or some non-state actor equipped with a swarm of RPAs possibly armed with WMD warheads. Perhaps centralized power is not the wave of the future. The highest social service any government can provide is preserving the physical security of its citizens. Governments have done this in large part through a monopoly of organized violence in armies and police forces. When large nation-states can no longer do that, will they pass from the scene?"[5] Wise words, indeed.

[5] Mets, 25.

Bibliography

Articles

PR Newswire. Unmanned Aerial Vehicle Market (Uav) Worth $114.7b by 2023. February 13, 2014. Accessed April 13, 2014. http://www.prnewswire.com/news-releases/unmanned-aerial-vehicle-market-uav-worth-1147b-by-2023-245370591.html.

Atherton, Kelsey "Senate Hearing: Drones Are 'Basically Flying Smartphones'." *Popular Science*, 21 March 2013. Accessed April 16, 2014. http://www.popsci.com/technology/article/2013-03/how-drone-smartphone.

Bowden, Mark. "How the Predator Drone Changed the Character of War." *Smithsonian Magazine*, November 2013. Accessed April 9, 2014. http://www.smithsonianmag.com/history/how-the-predator-drone-changed-the-character-of-war-3794671/?all.

Caraway, Bill. "Korea in the Eye of the Tiger: Ch. 5 Koryo and the Mongols, Building an Empire." Korean History Project. April 12, 2014. Accessed April 12, 2014.http://www.koreanhistoryproject.org/index.htm.

Christie, John. "Dod On a Glidepath to Bankruptcy." *Proceedings Magazine, US Naval Institute*134 (June 2008): 1. Accessed April 17, 2014. http://usni.org/magazines/proceedings/2008-06/dod-glide-path-bankruptcy.

Garamore, Jim. "From U.S. Civil War to Afghanistan: A Short History of UAVs." Defense.gov. April 16, 2002. Accessed April 8, 2014. http://www.defense.gov/news/newsarticle.aspx?id=44164.

Gaub, Darin MAJ. "Unready to Stop Uavs: It's Time to Get Serious About Countering Unmanned Enemy Aircraft." *Armed Forces Journal* 149, no. 5 (December 1, 2011): 1. Accessed April 16, 2014. http://www.armedforcesjournal.com/unready-to-stop-uavs/.

Gips, Michael. "A Remote Threat." *Security Management Online Archive*, October 2002. Accessed April 13, 2014 http://www.securitymanagement.com/library/001324.html.

Nicas, Jack. "FAA Unswayed by Do-Good Drones." *The Wall Street Journal*, April 6, 2014. Accessed April 17, 2014. http://online.wsj.com/news/articles/SB10001424052702303847804579481281535674284.

Sabatini, Nick. Federal Aviation Administration. "Federal Register: Unmanned Aircraft Operations in the National Airspace System, Docket No. Faa-2006-25714.." February 6, 2007. Accessed April 17, 2014. http://www.gpo.gov/fdsys/pkg/FR-2007-02-13/html/E7-2402.htm.

Singer, P.W. "Will Foreign Drones One Day Attack the U.S.?" *Newsweek*, March 13, 2010. Accessed April 17, 2014. http://www.newsweek.com/will-foreign-drones-one-day-attack-us-75331.

Sohn, Emily. "Model Airplane Flies the Atlantic." Student Science. December 15, 2003. Accessed April 17, 2014. https://student.societyforscience.org/article/model-plane-flies-atlantic.

Wass de Czege, Huba and Biever, Jacob, “Force Protections: from Fort to Foxhole, *Army Magazine* 51, no. 6 (June 2001).

http://www.ausa.org/publications/armymagazine/archive/2001/6/Documents/FC_de_Czege_0601.pdf, accessed 18 March 2014.

Books

Augustine, Norman R. *Augustine's Laws*. 6th ed. Reston, Va.: American Institute of Aeronautics and Astronautics, 1997.

Brugioni, Dino A. *Eyes in the Sky: Eisenhower, the Cia, and Cold War Aerial Espionage*. Edited by Doris G. Taylor. Annapolis, Md.: Naval Institute Press, 2010.

Clausewitz, Carl von. *On War*. Translated by Michael Howard, Peter Paret, and Bernard Brodie. Princeton, N.J.: Princeton University Press, 1984.

Clodfelter, Mark *The Limits of Air Power: The American Bombing of North Vietnam*. Lincoln: University of Nebraska Press, 2006.

Cronin, Audrey Kurth. *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns*. Princeton, N.J.: Princeton University Press, 2011.

Dolman, Everett C. *Astropolitik: Classical Geopolitics in the Space Age*. Cass Series--strategy and History. London: Frank Cass, 2002.

Friedman, Richard S. *Advanced Technology Warfare: A Detailed Study of the Latest Weapons and Techniques for Warfare Today and Into the 21st Century*. American ed. New York: Harmony Books, 1985.

Hoffman, David E. *The Dead Hand: The Untold Story of the Cold War Arms Race and Its Dangerous Legacy*. New York: Anchor Books, 2010.

Kalyvas, Stathis N. *The Logic of Violence in Civil War*. Cambridge Studies in Comparative Politics. Cambridge: Cambridge University Press, 2006.

Kilcullen, David *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*. New York: Oxford University Press, 2011, 2009.

McDougall, Walter A. *The Heavens and the Earth: A Political History of the Space Age*. Johns Hopkins paperbacks ed. Baltimore, Md.: Johns Hopkins University Press, 1997.

Mearsheimer, John J. *The Tragedy of Great Power Politics*. The Norton Series in World Politics. New York: Norton, 2001.

Mrozek, Donald. *Airpower and the Ground War in Vietnam: Ideas And*. Maxwell Air Force Base: Air University Press, 1988.

Overy, R J. *The Air War, 1939-1945*. Potomac ed. Cornerstones of Military History. Washington, DC: Potomac Books, Inc., 2005.

Shimko, Keith L. *The Iraq Wars and America's Military Revolution*. New York, NY: Cambridge University Press, 2010.

Shlapak, David A., and Alan Vick. *Check Six Begins On the Ground: Responding to the Evolving Ground Threat to Us Air Force*. Santa Monica, CA: RAND, 1995.

Singer, P W. *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century*. New York: Penguin Press, 2009.

Verhovek, Sam Howe. *Jet Age: The Comet, the 707, and the Race to Shrink the World*. New York: Avery, 2010.

Vick, Alan. *Snakes in the Eagle's Nest: A History of Ground Attacks On Air Bases*. Santa Monica, CA: Rand, 1995.

Waltz, Kenneth N. *Man, the State, and War: A Theoretical Analysis*. New York: Columbia University Press, 2001.

Government Publications

US Department of the Air Force, *Integrated Defense*, Air Force Policy Directive 31-1, (Washington, DC: U.S. Department of the Air Force, October 28, 2011).
US Department of the Army, *Operations*, Field Manual (FM) 3-0, (Washington, DC: U.S. Department of the Army, February 2008).
US Joint Chiefs of Staff, *Joint Security Operations in Theater*, Joint Publication 3-10 (Washington, DC: US Joint Chiefs of Staff, February 3, 2010)

Personal Communication – Interviews / E-Mails

Kifer, Michael. Deputy Director, PACAF A/7S, emails with author.

Reports and Testimonies

Bolkcom, Christopher. Senate testimony of Christopher Bolkcom, Analyst in National Defense for the Congressional Research Service before the Senate Governmental Affairs Committee, Subcommittee on International Security, Proliferation, and Federal Services.
Dillingham, Gerald. House, testimony of Gerald Dillingham, Director of Physical Infrastructure Issues, Government Accountability Office before the House Homeland Security Subcommittee on Oversight, Investigations and Management Hearing.
Gormley, Dennis. House, testimony of Dennis M. Gormley, Monterey Institute's Center for Nonproliferations Studies before the Subcommittee on National Security, Emerging Threats, and International Affairs, US House of Representatives Committee on Government Reform
Mets, David. "RPAs: Revolution or Retrogression." *Air Force Research Institute Papers* (paper 2010-1, April 2010): 1-25.
Miasnikov, Eugene. "Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects."*Center for Arms Control, Energy and Environmental Studies, Moscow Institute of Physics and Technology* (2005): 1.
Miller, Patrick. "Mini, Micro, and Swarming Unmanned Aerial Vehicles: A Baseline Study."*Library of Congress* (November 2006): 21.

Student Theses

Gray, Ron. "Integrated Swarming Operations for Air Base Defense: Applications in Irregular Warfare," Naval Postgraduate School, 2006.
Palmer, Glenn. "Air Base Security Operations: An Air Component Responsibility," School of Advanced Air and Space Studies, June 2006.
Sagraves, Robert D. "Airbase Defense Outside the Wire: Air Support for Defending Expeditionary Air Bases on the Nonlinear Battlefield," School of Advanced Air and Space Studies, June 2006.

Websites

"Arduplane." DIY Drones. April 17, 2014. Accessed April 17, 2014. https://code.google.com/p/ardupilot-mega/.

"At Home War Production." PBS.org. April 10, 2014. Accessed April 10, 2014 http://www.pbs.org/thewar/at_home_war_production.htm.

"Burrito Bomber." Darwin Aerospace. April 17, 2014. Accessed April 17, 2014. http://www.darwinaerospace.com/burritobomber.

"Drone Delivers Beer at Oppikoppi." News24.com. August 8, 2013. Accessed April 17, 2014.http://www.news24.com/Technology/News/Drone-delivers-beer-at-Oppikoppi-20130808.

"GPS Equipped Radio Controlled Sailplane HOWTO." April 12, 2014. Accessed April 12, 2014 http://jeklink.net/projects/GPS_Equipped_Radio_Controlled_Sailplane.html).

"Moore's Law -- or -- How Overall Processing Power for Computers Will Double Every Two Years." Moore's Law. April 18, 2014. Accessed April 18, 2014.http://www.mooreslaw.org/.

"Piccolo Autopilots: The Standard in Uas Systems." Cloud Cap Technology. April 13, 2014. Accessed April 13, 2014. http://www.cloudcaptech.com/piccolo_system.shtm.

"Rmax Type IIG/Type II History." Yamaha RMAX History. April 8, 2014. Accessed April 15, 2014. http://rmax.yamaha-motor.com.au/history.

"UAV Flight Systems Autopilot Products.." April 15, 2014. Accessed April 15, 2014.http://www.chinaga.com/bank/896.pdf.